PATENT ABSTRACTS OF JAPAN

(11)Publication number : **11-112950**
(43)Date of publication of application : **23.04.1999**

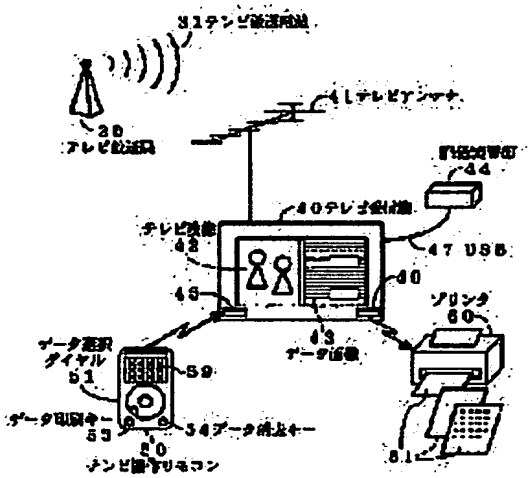
(51)Int.Cl. H04N 7/08
H04N 7/081
H04H 1/00
H04L 9/08
H04L 9/36
// H04N 7/167

(21)Application number : **09-274151**
(22)Date of filing : **07.10.1997**

(71)Applicant : **FUJI XEROX CO LTD**
(72)Inventor : **ICHIMURA SATORU**

(54) ENCRYPTION INFORMATION DECODING REPRODUCING DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To distribute in advance encryption information, that is known to only those persons who viewed a television program prior to broadcasting of the television program.
SOLUTION: A broadcast station broadcasts encryption data to be decoded in interlocking with a television program, prior to start of the television program together with program identification information to specify the encryption data. A receiver receives the encryption data and stores the data to an encryption information storage section 6. The broadcast station sends a decoding key to decode the encryption data, in matching with a progress of the program. When a viewer views the program, the receiver receives the decoding key and an encryption information decoding section 9 decodes the encryption data stored in the encryption information storage section 6 by using the decoding key. The decoded encryption data are processed by an encryption information reproduction section 10 and displayed together with a television video image.



LEGAL STATUS

[Date of request for examination] 20.08.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision

of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－112950

(43)公開日　平成11年(1999)４月23日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０４Ｎ	7/08	Ｈ０４Ｎ	7/08	Ｚ
	7/081	Ｈ０４Ｈ	1/00	Ｆ
Ｈ０４Ｈ	1/00	Ｈ０４Ｌ	9/00	６０１Ｚ
Ｈ０４Ｌ	9/08			６０１Ｅ
	9/36			６８５

審査請求　未請求　請求項の数14　ＯＬ　（全 28 頁）　最終頁に続く

(21)出願番号　特願平9－274151

(22)出願日　平成９年(1997)10月７日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72)発明者　市村　哲
神奈川県足柄上郡中井町境430　グリーンテクなか　い　富士ゼロックス株式会社内

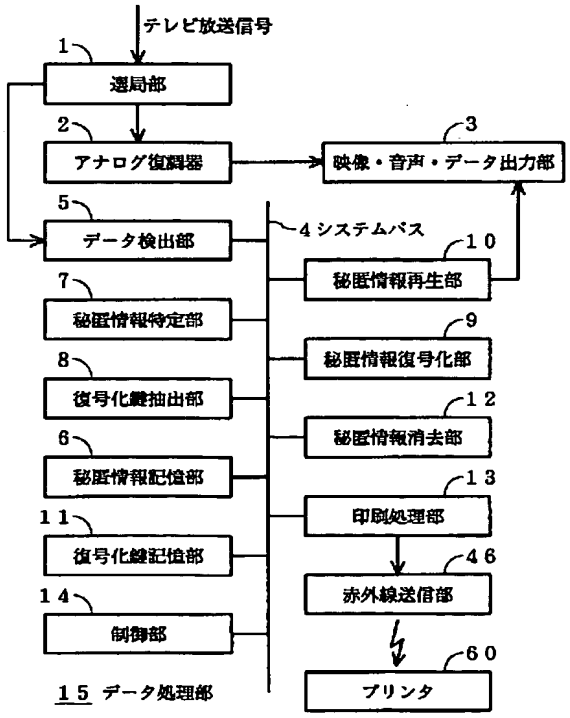
(74)代理人　弁理士　佐藤　正美

(54)【発明の名称】　秘匿情報復号再生装置

(57)【要約】

【課題】　テレビ番組を視聴した人だけが知ることができる秘匿情報をテレビ番組の放送に先立って予め配信することができるようにする。

【解決手段】　放送局は、テレビ番組の開始に先立って、その番組と連動して復号化されるべき、暗号化された秘匿データを、それを特定するための番組識別情報などとともに、放送する。受信機は、その秘匿データを受信して、秘匿情報記憶部６に記憶する。放送局は、番組の進行に合わせて、秘匿データを復号化できる復号化鍵を送信する。視聴者が番組を見ていれば、受信機は、その復号化鍵を受信して、秘匿情報復号化部９で、秘匿情報記憶部６に記憶されている秘匿データを、その復号化鍵によって復号化する。復号化された秘匿データは、秘匿情報再生部１０によって処理されて、テレビ映像とともに表示される。



1

【特許請求の範囲】

【請求項１】暗号化された情報を秘匿情報として記憶する秘匿情報記憶手段と、

テレビ放送信号またはラジオ放送信号の映像情報または音声情報である映像音声情報を受信する映像音声情報受信手段と、

この映像音声情報受信手段によって受信された映像音声情報を再生する映像音声情報再生手段と、

前記テレビ放送信号またはラジオ放送信号に重畳されたデータを検出するデータ検出手段と、

このデータ検出手段によって検出されたデータに含まれる情報に基づいて、前記秘匿情報記憶手段に記憶された秘匿情報のうちの、前記映像音声情報が再生されるのに伴って復号化されるべき秘匿情報を特定する秘匿情報特定手段と、

前記データ検出手段によって検出されたデータに含まれる情報から、前記秘匿情報特定手段によって特定された秘匿情報を復号化するための復号化鍵を抽出する復号化鍵抽出手段と、

前記秘匿情報記憶手段に記憶された秘匿情報のうちの、前記秘匿情報特定手段によって特定された秘匿情報を、前記復号化鍵抽出手段によって抽出された復号化鍵によって復号化する秘匿情報復号化手段と、

この秘匿情報復号化手段によって復号化された秘匿情報を、前記映像音声情報が再生されるのに伴って再生する秘匿情報再生手段と、

を備えることを特徴とする秘匿情報復号再生装置。

【請求項２】請求項１の秘匿情報復号再生装置において、

前記秘匿情報記憶手段に記憶される秘匿情報は、当該秘匿情報を復号化するための復号化鍵が前記復号化鍵抽出手段によって抽出される時点より前の時点において、前記テレビ放送信号またはラジオ放送信号に重畳されて放送されて、前記データ検出手段によって検出されたものであることを特徴とする秘匿情報復号再生装置。

【請求項３】請求項１の秘匿情報復号再生装置において、

前記秘匿情報記憶手段は、暗号化された情報が秘匿情報として書き込まれた外部記憶装置であることを特徴とする秘匿情報復号再生装置。

【請求項４】請求項１～３のいずれかの秘匿情報復号再生装置において、

当該秘匿情報復号再生装置は、さらに復号化鍵記憶手段を備え、

その復号化鍵記憶手段は、前記復号化鍵抽出手段によって抽出された復号化鍵と、この復号化鍵によって復号化可能な前記秘匿情報記憶手段に記憶された秘匿情報を特定する特定情報とを、互いに対応づけて記憶し、

前記秘匿情報復号化手段は、前記秘匿情報記憶手段に記憶された秘匿情報のうちの、前記復号化鍵記憶手段に記憶された特定情報によって特定された秘匿情報を、前記復号化鍵記憶手段に記憶された復号化鍵によって復号化することを特徴とする秘匿情報復号再生装置。

2

【請求項５】請求項１～４のいずれかの秘匿情報復号再生装置において、

前記秘匿情報特定手段は、前記データ検出手段によって検出されたデータに含まれる放送番組識別情報によって、前記映像音声情報が再生されるのに伴って復号化されるべき前記秘匿情報記憶手段に記憶された秘匿情報を特定することを特徴とする秘匿情報復号再生装置。

【請求項６】請求項１～４のいずれかの秘匿情報復号再生装置において、

前記秘匿情報特定手段は、前記データ検出手段によって検出されたデータに含まれる放送局識別情報と、この放送局識別情報を含むデータが前記データ検出手段によって検出されたタイミングとに基づいて、前記映像音声情報が再生されるのに伴って復号化されるべき前記秘匿情報記憶手段に記憶された秘匿情報を特定することを特徴とする秘匿情報復号再生装置。

【請求項７】請求項１～６のいずれかの秘匿情報復号再生装置において、

前記秘匿情報復号化手段は、前記秘匿情報記憶手段に記憶された秘匿情報のうちの、前記秘匿情報特定手段によって特定された秘匿情報を、前記復号化鍵抽出手段によって抽出された復号化鍵と、外部メモリ装置に記憶された第２の復号化鍵とによって復号化することを特徴とする秘匿情報復号再生装置。

【請求項８】請求項７の秘匿情報復号再生装置において、

前記第２の復号化鍵は、視聴者または秘匿情報復号再生装置が前記秘匿情報特定手段によって特定された秘匿情報を復号化する権利を有するか否かを識別するために用いられる鍵であって、視聴者または秘匿情報復号再生装置が前記権利を有する場合には、前記復号化鍵抽出手段によって抽出された復号化鍵と、当該第２の復号化鍵とによって、前記秘匿情報特定手段によって特定された秘匿情報を正しく復号化できるものであることを特徴とする秘匿情報復号再生装置。

【請求項９】請求項８の秘匿情報復号再生装置において、

前記秘匿情報記憶手段に記憶される秘匿情報が、視聴者または秘匿情報復号再生装置ごとに異なる個別暗号化鍵と、全視聴者または全秘匿情報復号再生装置に共通の共通暗号化鍵とによって暗号化されたものであることを特徴とする秘匿情報復号再生装置。

【請求項１０】請求項１～６のいずれかの秘匿情報復号再生装置において、

前記復号化鍵抽出手段によって抽出される復号化鍵は、暗号化されたものであり、

前記秘匿情報復号化手段は、この復号化鍵抽出手段によ

って抽出された復号化鍵を、外部メモリ装置に記憶された第２の復号化鍵によって復号化し、その復号化された復号化鍵によって、前記秘匿情報記憶手段に記憶された秘匿情報のうちの、前記秘匿情報特定手段によって特定された秘匿情報を復号化することを特徴とする秘匿情報復号再生装置。

【請求項１１】請求項１０の秘匿情報復号再生装置において、

前記第２の復号化鍵は、視聴者または秘匿情報復号再生装置が前記秘匿情報特定手段によって特定された秘匿情報を復号化する権利を有するか否かを識別するために用いられる鍵であって、視聴者または秘匿情報復号再生装置が前記権利を有する場合には、前記復号化鍵抽出手段によって抽出された復号化鍵を、当該第２の復号化鍵によって正しく復号化できるものであることを特徴とする秘匿情報復号再生装置。

【請求項１２】請求項１～６のいずれかの秘匿情報復号再生装置において、

当該秘匿情報復号再生装置は、さらに暗号化鍵検出手段と暗号化鍵記憶手段とを備え、

前記秘匿情報記憶手段に記憶される秘匿情報は、第１の暗号化鍵によって暗号化されたものであり、

前記暗号化鍵検出手段は、前記第１の暗号化鍵が第２の暗号化鍵と第３の暗号化鍵とによって暗号化されて、前記テレビ放送信号またはラジオ放送信号に重畳されて放送された暗号化鍵情報を検出し、

前記暗号化鍵記憶手段は、この暗号化鍵検出手段によって検出された暗号化鍵情報を、前記秘匿情報記憶手段に記憶された秘匿情報と対応づけて記憶し、

前記復号化鍵抽出手段は、前記秘匿情報特定手段によって特定された秘匿情報を復号化するための復号化鍵として前記第３の暗号化鍵を抽出し、

前記秘匿情報復号化手段は、この復号化鍵抽出手段によって抽出された第３の暗号化鍵と、外部メモリ装置に記憶された、視聴者または秘匿情報復号再生装置ごとに異なる第２の復号化鍵とによって、前記暗号化鍵記憶手段に記憶された暗号化鍵情報を復号化して、前記第１の暗号化鍵を抽出するとともに、この抽出した第１の暗号化鍵を復号化鍵として、前記秘匿情報特定手段によって特定された秘匿情報を復号化することを特徴とする秘匿情報復号再生装置。

【請求項１３】請求項１～６のいずれかの秘匿情報復号再生装置において、

当該秘匿情報復号再生装置は、さらに暗号化鍵検出手段と暗号化鍵記憶手段とを備え、

前記秘匿情報記憶手段に記憶される秘匿情報は、第１の暗号化鍵によって暗号化されたものであり、

前記暗号化鍵検出手段は、前記第１の暗号化鍵が第３の暗号化鍵によって暗号化され、さらにその暗号化された情報が第２の暗号化鍵によって暗号化されて、前記テレビ放送信号またはラジオ放送信号に重畳されて放送された暗号化鍵情報を検出し、

前記暗号化鍵記憶手段は、この暗号化鍵検出手段によって検出された暗号化鍵情報が、外部メモリ装置に記憶された、視聴者または秘匿情報復号再生装置ごとに異なる第２の復号化鍵によって復号化された暗号化鍵情報を、前記秘匿情報記憶手段に記憶された秘匿情報と対応づけて記憶し、

前記復号化鍵抽出手段は、前記秘匿情報特定手段によって特定された秘匿情報を復号化するための復号化鍵として前記第３の暗号化鍵を抽出し、

前記秘匿情報復号化手段は、この復号化鍵抽出手段によって抽出された第３の暗号化鍵によって、前記暗号化鍵記憶手段に記憶された暗号化鍵情報を復号化して、前記第１の暗号化鍵を抽出するとともに、この抽出した第１の暗号化鍵を復号化鍵として、前記秘匿情報特定手段によって特定された秘匿情報を復号化することを特徴とする秘匿情報復号再生装置。

【請求項１４】請求項１２または１３の秘匿情報復号再生装置において、

前記第１の暗号化鍵が、全視聴者または全秘匿情報復号再生装置に共通のものであり、前記第２の暗号化鍵が、視聴者または秘匿情報復号再生装置ごとに異なるものであり、前記第３の暗号化鍵が、全視聴者または全秘匿情報復号再生装置に共通のものであることを特徴とする秘匿情報復号再生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、テレビ放送またはラジオ放送を受信し、受信したテレビまたはラジオの映像または音声と関連する暗号化された秘匿情報を、テレビまたはラジオの映像または音声の再生タイミングに合わせて復号化して、テレビまたはラジオの映像または音声に伴って再生する装置に関する。なお、この明細書では、「テレビジョン」を「テレビ」と称する。

【０００２】

【従来の技術】従来のインターネットは、ユーザが自分の欲しい情報を能動的に取りに行くという利用形態で用いられることが多い。この利用形態は、「ＰＵＬＬ型」と呼ばれている。これに対して、ユーザが情報を能動的に取りに行くのではなく、放送局からユーザに対してデータが次々と送られてくる「ＰＵＳＨ型」の利用形態でインターネットが用いられることが増えてきた。ＰＵＳＨ型サービスで送られたデータは、ユーザのパソコン表示画面上に次々と表示される。

【０００３】しかしながら、一般家庭でインターネットを利用する場合には、電話回線をインターネットプロバイダに接続する場合が多い。そのため、放送局から随時送られてくるＰＵＳＨ型データを受信するには、電話をインターネットプロバイダに常時かけっぱなしにする必

要があり、電話代が非常に高額になるという問題がある。

【０００４】一方、地上波テレビ放送信号の垂直帰線消去期間（ＶＢＩ）を利用してＨＴＭＬ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｍａｋｅｕｐ　Ｌａｎｇｕａｇｅ）書式のインターネットデータを重畳して放送する「Ｗｅｂキャスト」（出典：インターネットアスキー、Ｖｏｌ．２，Ｎｏ．５，ｐｐ．１６６－１６７，１９９７年５月号）が米国で開始されている。日本では１９９６年４月から、地上波テレビ放送信号の２１ライン分の垂直帰線消去期間中の４ラインがデータ多重放送として割り当てられ、この４ラインの伝走路によってＷｅｂキャストが行われている。

【０００５】また、衛星デジタルテレビ放送でも、デジタル化した映像情報および音声情報にＨＴＭＬ書式のインターネットデータを重畳して放送する試みが開始されている。デジタルテレビ放送の場合には、映像情報、音声情報およびデータの三者を統一的にデジタル情報として扱えるので、垂直帰線消去期間を利用することなくインターネットデータをテレビ電波で放送することができる。

【０００６】そして、地上波テレビ放送や衛星デジタルテレビ放送に重畳されて放送されるインターネットデータを受信する場合には、電話回線を用いる必要がないため、放送局から随時送られてくるＰＵＳＨ型データを非常に安価に常時受信することができる利点がある。

【０００７】さらに、データをテレビ放送に重畳する場合には、テレビ映像とデータを連動させてユーザに配信することができる利点がある。これによって、テレビ番組と関連のあるデータを配信することができ、例えば、教育番組などの映像と同時に教材テキストなどのデータを配信して、テレビ画面やパソコン画面にマルチウィンドウで表示する、といった使い方が可能になる。また、テレビ放送の内容や話題が変わるたびに新たなデータを放送することによって、内容や話題に追従してデータ内容を変えることができるようになる。

【０００８】また、日本で放送開始が計画されているＢｉｔｃａｓｔ／ＶＢＩサービス（出典：日経マルチメディア、ｐｐ．５２－５９，１９９７年４月号）の受信機を利用する場合には、テレビ放送によって送信されたインターネットデータを受信機の記憶装置に一旦蓄積しておき、その蓄積されたインターネットデータを放送番組と連動させて表示することができる。すなわち、テレビ番組やテレビコマーシャルと連動するデータを予めデータ放送によって放送しておき、そのテレビ番組やテレビコマーシャルが始まった瞬間に画面上に表示させることができる。

【０００９】

【発明が解決しようとする課題】ところで、Ｗｅｂページ（インターネットデータ）の中には、情報提供者によって許可された人以外の人は見ることができないようにされているページがある。一般的には、これらの秘匿Ｗｅｂページにはパスワードが設定され、このパスワードを知る人のみが、その秘匿Ｗｅｂページにアクセスできるようになっている。

【００１０】このように、ユーザが自分の欲しい情報を能動的に取りに行くという「ＰＵＬＬ型」の利用形態でインターネットを利用する場合には、情報提供者は、秘匿したいＷｅｂページにパスワードを設定することによって、適切なユーザからのアクセスのみを許すＷｅｂページをインターネット上に公開することができる。

【００１１】そこで、テレビ映像と連動して表示されるべきＷｅｂページについても、情報提供者が許可した視聴者にだけアクセスを許すＷｅｂページを放送または公開することができれば、非常に便利である。例えば、秘匿Ｗｅｂページをテレビ番組の開始時刻に先立って放送し、情報提供者が許可した視聴者だけがテレビ番組の進行に合わせて、その秘匿Ｗｅｂページを読み出して見ることができるようにする、というものである。

【００１２】しかしながら、前述のＢｉｔｃａｓｔ／ＶＢＩサービスのように、ＰＵＳＨ型サービスによってデータを配信する場合には、受信機の記憶装置に蓄積されたデータは、誰もが、いつでも見ることができるため、適切なユーザからのアクセスのみを許すＷｅｂージを、テレビ番組の放送時刻に先立って予め配信しておくことはできないという問題がある。

【００１３】公知の暗号技術を利用して、この問題を解決する方法として、放送局は、テレビ番組に関連したデータを暗号化して放送し、受信機では、その暗号化データを受信して記憶装置に記憶し、視聴者は、その記憶された暗号化データを別途、電子メールや郵便はがきによって放送局から送られた復号化鍵（パスワードなど）を用いて復号化する、という方法が考えられる。

【００１４】例えば、放送局から送られる電子メールや郵便はがきに、復号化鍵のほかに、その復号化鍵を利用できる放送番組名が書かれていれば、復号化鍵を入手した視聴者は、放送局によって指定された放送番組に関連する暗号化データのみを復号化することができる。

【００１５】しかしながら、この方法の場合、テレビ番組と連動して再生されるべき秘匿データを再生するためには、視聴者は、受信機の記憶装置に記憶された暗号化データの中から、当該テレビ番組に関連する暗号化データを検索し、その検索した暗号化データを、電子メールや郵送によって放送局から送られた復号化鍵によって復号化する必要があり、この操作のために、視聴しているテレビ番組に集中できないという問題がある。

【００１６】しかも、同一のテレビ番組内であっても、番組の進行または秘匿データの内容に応じて、秘匿データを視聴できる人を動的に変えたい場合もあり、このような場合には、放送局から予め電子メールや郵送によっ

て復号化鍵を送付しておくことは極めて困難であるという問題もある。

【００１７】さらに、電子メールや郵送によって放送局から送られた復号化鍵によって暗号化データを復号化する場合には、視聴者は復号化鍵を入手した時点以降のタイミングであれば、いつでも暗号化データを復号化できてしまうために、テレビ番組と連動して再生されるべき秘匿データをテレビ番組の放送開始以前のタイミングでは視聴できないようにするなどの、時間制限を付けたアクセス制御をすることができないという問題がある。

【００１８】また、特開平９－１３９９３３号公報には、秘匿データを保持するデータベースにアクセスするための方法として、放送局が、データベースアクセスのための案内情報をテレビ映像に重畳して放送し、視聴者は、その受信したデータベースアクセスのための案内情報と、視聴者自身が知るパスワードとを入力して、電話回線を通じてデータベースにアクセスすることにより、秘匿データを入手する方法が示されている。

【００１９】しかしながら、この方法は、電話回線を使用する必要があるので、通信コストがかかるという問題がある。また、電話回線に接続するための通信装置を備える必要があるため、テレビ受信システムが複雑になるという問題がある。さらに、この場合に視聴者が入力すべきパスワードは別途、電子メールや郵送によって入手する必要があり、前述したように手間がかかるという問題がある。

【００２０】ところで、テレビコマーシャルを視聴者に見てもらう方法の一つとして、スポンサーが提供するテレビ番組を見た視聴者だけに、そのスポンサーからのプレゼントを送る場合があるが、同様にテレビ番組を見た視聴者だけに、有益な情報や特別の権利を提供することによって、スポンサーが放送したテレビコマーシャルをより多くの視聴者に見てもらうことができる。

【００２１】例えば、テレビ番組と連動して動作するコンピュータプログラムを予め放送しておき、テレビ番組を見た視聴者だけに、そのコンピュータプログラムを実行する権利を与えるようにすることができれば、コンピュータプログラムを実行したい視聴者がテレビ番組を見るようになるので、テレビコマーシャルを視聴者に見てもらう方法として、非常に有益である。

【００２２】しかしながら、前述したように、ＰＵＳＨ型サービスによってデータを配信する場合には、受信機の記憶装置に蓄積されたデータは、誰もが、いつでも見ることができるため、テレビ番組を見た視聴者だけにアクセスを許すＷｅｂページを、テレビ番組の放送時刻に先立って予め配信しておくことはできないという問題がある。

【００２３】日本国内で放送が開始されている衛星デジタルテレビ放送「ＰｅｒｆｅｃＴＶ！」では、スクランブル映像と、このスクランブル映像を復号化するための復号化鍵とを同時に放送するようになっているが、この場合にも、テレビ番組で使用するデータやプログラムを、テレビ番組の放送時刻に先立って予め視聴者に配信しておくことはできない。

【００２４】すなわち、ＰｅｒｆｅｃＴＶ！の場合には、テレビ番組と連動して復号化されるべき秘匿データが大量に存在する場合でも、秘匿データを利用するタイミングで秘匿データを放送する必要がある。さらに、同一の秘匿データを複数の場面または番組で利用する場合でも、放送局は秘匿データを利用するタイミングで毎回、当該秘匿データを放送しなければならないという問題がある。

【００２５】さらに、ＰｅｒｆｅｃＴＶ！の場合には、スクランブル映像と、このスクランブル映像を復号化するための復号化鍵とを同時に配信するようになっているため、ＣＤＲＯＭなどの放送以外のメディアによって視聴者に提供された秘匿データを、テレビ番組と連動させて復号化し、再生するというようなことができないという問題がある。

【００２６】以上の点から、この発明は、（１）テレビまたはラジオの番組を視聴した人だけが知ることができる秘匿情報を番組の放送に先立って予め配信することができ、（２）テレビまたはラジオの番組に関連した秘匿情報を不特定多数の視聴者に対して配信する場合でも、特定の視聴者だけに情報を知る権利を与えることができ、（３）テレビまたはラジオの番組の進行に合わせて、情報の公開・非公開、または情報を知ることができる視聴者を動的に変更することができ、（４）視聴者が秘匿情報を復号化する操作を強いられず、視聴しているテレビまたはラジオの番組に集中することができ、（５）同一の秘匿情報を複数の場面または番組で利用する場合には、一度配信した秘匿情報を再利用することができ、（６）ＣＤＲＯＭなどの放送以外のメディアによって視聴者に提供された秘匿情報でも、テレビまたはラジオの番組に連動させて復号化して再生することができる、ようにすることにある。

【００２７】

【課題を解決するための手段】この発明では、秘匿情報復号再生装置として、暗号化された情報を秘匿情報として記憶する秘匿情報記憶手段と、テレビ放送信号またはラジオ放送信号の映像情報または音声情報である映像音声情報を受信する映像音声情報受信手段と、この映像音声情報受信手段によって受信された映像音声情報を再生する映像音声情報再生手段と、前記テレビ放送信号またはラジオ放送信号に重畳されたデータを検出するデータ検出手段と、このデータ検出手段によって検出されたデータに含まれる情報に基づいて、前記秘匿情報記憶手段に記憶された秘匿情報のうちの、前記映像音声情報が再生されるのに伴って復号化されるべき秘匿情報を特定する秘匿情報特定手段と、前記データ検出手段によって検

出されたデータに含まれる情報から、前記秘匿情報特定手段によって特定された秘匿情報を復号化するための復号化鍵を抽出する復号化鍵抽出手段と、前記秘匿情報記憶手段に記憶された秘匿情報のうちの、前記秘匿情報特定手段によって特定された秘匿情報を、前記復号化鍵抽出手段によって抽出された復号化鍵によって復号化する秘匿情報復号化手段と、この秘匿情報復号化手段によって復号化された秘匿情報を、前記映像音声情報が再生されるのに伴って再生する秘匿情報再生手段と、を設ける。

【００２８】この場合、前記秘匿情報記憶手段に記憶される秘匿情報は、当該秘匿情報を復号化するための復号化鍵が前記復号化鍵抽出手段によって抽出される時点より前の時点において、前記テレビ放送信号またはラジオ放送信号に重畳されて放送されて、前記データ検出手段によって検出されたものとすることができる。

【００２９】あるいはまた、前記秘匿情報記憶手段は、暗号化された情報が秘匿情報として書き込まれた外部記憶装置とすることができる。

【００３０】なお、この明細書では、暗号化された情報だけでなく、その暗号化された情報を復号化した情報も、便宜上、秘匿情報と称する。

【００３１】

【作用】上記のように構成した、この発明の秘匿情報復号再生装置においては、放送局がテレビまたはラジオの番組の放送に先立って予め、その番組と連動して復号化されるべき秘匿情報を放送することによって、番組放送前に、その番組と連動して復号化されるべき秘匿情報が、秘匿情報記憶手段に記憶されるようになる。あるいはまた、放送局が番組の放送に先立って予め、その番組と連動して復号化されるべき秘匿情報が書き込まれた、ＣＤＲＯＭなどの外部記憶装置を視聴者に配布することによって、秘匿情報記憶手段は、番組放送前に、その番組と連動して復号化されるべき秘匿情報を記憶した状態となる。

【００３２】このように秘匿情報記憶手段に秘匿情報が記憶された状態で、番組開始とともに放送局が、当該番組の映像情報または音声情報が再生されるのに伴って復号化されるべき秘匿情報を特定することができる、放送番組識別情報などの情報と、これによって特定される秘匿情報を復号化するための復号化鍵とを放送することによって、秘匿情報復号再生装置においては、秘匿情報特定手段によって、秘匿情報記憶手段に記憶された秘匿情報のうちの、当該番組の映像情報または音声情報が再生されるのに伴って復号化されるべき秘匿情報が特定され、復号化鍵抽出手段によって、その特定された秘匿情報を復号化するための復号化鍵が抽出され、秘匿情報復号化手段によって、その特定された秘匿情報が、その抽出された復号化鍵によって復号化され、秘匿情報再生手段によって、その復号化された秘匿情報が、当該番組の映像情報または音声情報が再生されるのに伴って、画像または音声として再生される。

【００３３】したがって、テレビまたはラジオの番組を視聴した人だけが知ることができる秘匿情報を番組の放送に先立って予め配信することができ、視聴者が秘匿情報を復号化する操作を強いられず、視聴しているテレビまたはラジオの番組に集中することができ、同一の秘匿情報を複数の場面または番組で利用する場合には、一度配信した秘匿情報を再利用することができるとともに、ＣＤＲＯＭなどの放送以外のメディアによって視聴者に提供された秘匿情報でも、テレビまたはラジオの番組に連動させて復号化して再生することができる。

【００３４】さらに、放送局で復号化鍵の送信や内容を調整することによって、テレビまたはラジオの番組の進行に合わせて、情報の公開・非公開、または情報を知ることができる視聴者を動的に変更することができるとともに、テレビまたはラジオの番組に関連した秘匿情報を不特定多数の視聴者に対して配信する場合でも、特定の視聴者だけに情報を知る権利を与えることができるようになる。

【００３５】

【発明の実施の形態】この発明の実施形態を、この発明をテレビ放送の送受信システムに適用した場合につき示す。ただし、後述するように、この発明はラジオ放送の送受信システムにも適用することができる。

【００３６】なお、「特許請求の範囲」および「課題を解決するための手段」では、「映像情報または音声情報」を「映像音声情報」と定義したが、以下の実施形態は、この発明をテレビ放送の送受信システムに適用した場合であるので、以下の実施形態では、「映像音声情報」は「映像情報および音声情報」を意味するものとする。

【００３７】［第１の実施形態］第１の実施形態では、放送局は、テレビ番組の開始に先立って予め、テレビ放送によって秘匿データを放送し、テレビ番組の進行に合わせて、先に放送した秘匿データを復号化するための復号化鍵を放送する。テレビ受信機を含む受信システムでは、先に放送された秘匿データを秘匿情報記憶部に記憶し、テレビ番組の進行に合わせて放送された復号化鍵を検出して、この復号化鍵によって秘匿情報記憶部に記憶された秘匿データを復号化して、画像または音声として表示または再生する。

【００３８】ただし、以下においては、秘匿データが画像として表示されるものである場合についてのみ示す。

【００３９】また、第１の実施形態は、この発明を地上波テレビ放送の送受信システムに適用した場合である。

【００４０】（構成）図１は、第１の実施形態の送受信システムの一例を示す。テレビ放送局３０は、テレビ放送電波３１によって、地上波テレビ放送として、変調されたアナログ映像音声信号を送信するとともに、例え

ば、テレビ映像信号の垂直帰線消去期間中の第１０ラインから第１３ラインまでの４ラインを利用して、秘匿データや復号化鍵などのデジタルデータを送信する。１ライン当たり９．６ｋｂｐｓの伝送容量があるので、４ライン分では３８．４ｋｂｐｓのデータを伝送することができる。

【００４１】この例の場合、送信されるデジタルデータは、ＨＴＭＬ書式のインターネットデータであり、秘匿データについては暗号化されたものである。典型的なインターネットデータは、レイアウト情報、プレーンテキスト、動画、静止画、音声、他のインターネットデータへのリンク情報、またはコンピュータプログラムを含む。

【００４２】受信システムは、全体として、テレビ受信機４０、テレビアンテナ４１、記憶装置部４４、テレビ操作リモコン５０、およびプリンタ６０を備え、テレビ放送局３０からの、変調されたアナログ映像音声信号、および秘匿データや復号化鍵などのデジタルデータを含むテレビ放送信号は、テレビアンテナ４１で受信されて、テレビ受信機４０内の選局部で選局される。

【００４３】テレビ受信機４０は、その表示画面上にテレビ映像４２とインターネットデータによるデータ画像４３とを同時に表示できるようにし、通常は、表示画面全体にテレビ映像４２を表示するが、秘匿データを受信して秘匿情報記憶部に記憶し、その後、この秘匿データを復号化するための復号化鍵を受信して、その復号化鍵によって秘匿情報記憶部に記憶されている秘匿データを復号化したときには、その復号化したインターネットデータによるデータ画像４３を、テレビ映像４２と同時に表示するようにする。

【００４４】テレビ映像４２とデータ画像４３とを同時に表示する方法としては、図示するように表示画面を横方向に２分割する方法以外に、いわゆるピクチャインピクチャ方式や、表示画面全体にテレビ映像４２を表示し、それにオーバーラップさせる形で、テレビ映像４２上の複数の領域に分散させてデータ画像４３を表示する方法などを用いることができる。さらに、テレビ受信機４０の表示部とは別の表示装置にデータ画像４３を表示するようにしてもよい。

【００４５】記憶装置部４４は、上記の秘匿情報記憶部および後述する復号化鍵記憶部を構成するもので、記憶媒体として、ハードディスク（磁気ディスク）、光磁気ディスク、フラッシュメモリなどを用い、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）４７によってテレビ受信機４０と接続する。これによって、テレビ受信機４０と記憶装置部４４との間では１２Ｍｂｐｓでデータを転送することができる。

【００４６】ただし、記憶装置部４４はテレビ受信機４０内に設置してもよい。また、記憶装置部４４の記憶媒体として、ＭＤ、ＺＩＰディスク、ＰＣＭＰＣＩＡ対応フラッシュメモリカードなどの交換可能な記録媒体を利用すれば、容易に記憶容量を増やすことができるようになる。

【００４７】テレビ操作リモコン５０は、テレビ受信機４０の赤外線受信部４５に赤外線リモコン信号を送信して、テレビ受信機４０を制御するもので、データ選択ダイヤル５１、データ印刷キー５３、データ消去キー５４、およびその他のキー群５９を有する。その他のキー群５９は、通常のテレビ操作リモコンが備える電源スイッチ、選局キー、音量調節キーなどである。

【００４８】データ選択ダイヤル５１は、これを回すことによって、記憶装置部４４の秘匿情報記憶部に記憶されている秘匿データから、再表示すべき秘匿データを選択するものである。後述するように、その選択された秘匿データは、記憶装置部４４の復号化鍵記憶部に記憶されている、その選択された秘匿データを復号化するための復号化鍵によって復号化されて、データ画像４３として再表示される。

【００４９】データ印刷キー５３は、秘匿データが復号化鍵によって復号化されて表示されているときに、またはデータ選択ダイヤル５１によって再表示すべき秘匿データを選択して再表示した状態で、これを押下することによって、その表示または再生された秘匿データをプリンタ６０によって用紙６１上に画像として印刷するものである。

【００５０】この場合、復号化された秘匿データは、テレビ受信機４０の赤外線送信部４６で赤外線信号とされてプリンタ６０に送信される。この赤外線伝送は、ＩｒＤＡ１．１規格に準拠したもので、４Ｍｂｐｓで印刷データを転送することができる。

【００５１】データ消去キー５４は、これを押下することによって、後述するように、記憶装置部４４の秘匿情報記憶部に記憶されている秘匿データを消去するものである。

【００５２】図２は、第１の実施形態の秘匿情報復号再生装置の機能ブロック構成を示す。この実施形態の秘匿情報復号再生装置は、選局部１、アナログ復調部２、映像・音声・データ出力部３、およびデータ処理部１５を備える。

【００５３】変調されたアナログ映像音声信号、および秘匿データや復号化鍵などのデジタルデータを含むテレビ放送信号は、選局部１で選局され、その選局されたテレビ放送信号中の変調されたアナログ映像音声信号が、アナログ復調部２で復調され、その復調されたアナログ映像音声信号が、映像・音声・データ出力部３に供給される。映像・音声・データ出力部３は、図１に示したテレビ受信機４０の表示部およびスピーカによって構成され、表示部の表示画面にテレビ映像およびデータ画像が表示され、スピーカからテレビ音声が再生される。

【００５４】データ処理部１５は、システムバス４に対

して、データ検出部５、秘匿情報記憶部６、秘匿情報特定部７、復号化鍵抽出部８、秘匿情報復号化部９、秘匿情報再生部１０、復号化鍵記憶部１１、秘匿情報消去部１２、印刷処理部１３、および制御部１４が、それぞれ接続されて構成される。

【００５５】ただし、データ処理部１５は、実装的には、１つのブロックが幾つかの機能部分を含むように、または１つの機能部分が幾つかのブロックに分割されるように、構成することができる。

【００５６】データ検出部５は、選局部１で選局されたテレビ放送信号中の、秘匿データや復号化鍵などのデジタルデータを検出して、システムバス４に出力する。

【００５７】秘匿情報記憶部６は、データ検出部５によって検出されたデータに含まれる秘匿データを記憶するもので、上述したように記憶装置部４４に設けられる。

【００５８】秘匿情報特定部７は、データ検出部５によって検出されたデータに含まれる後述する放送番組識別情報などの情報に基づいて、秘匿情報記憶部６に記憶された秘匿データのうちの、テレビの映像および音声が再生されるのに伴って復号化されるべき秘匿データを特定する。

【００５９】復号化鍵抽出部８は、データ検出部５によって検出されたデータに含まれる情報から、秘匿情報特定部７によって特定された秘匿データを復号化するための復号化鍵を抽出する。

【００６０】秘匿情報復号化部９は、秘匿情報記憶部６に記憶された秘匿データのうちの、秘匿情報特定部７によって特定された秘匿データを、復号化鍵抽出部８によって抽出された復号化鍵によって復号化する。

【００６１】秘匿情報再生部１０は、秘匿情報復号化部９によって復号化された秘匿データ、すなわち、この例ではＨＴＭＬ書式のインターネットデータを、表示するように処理して、映像・音声・データ出力部３に出力する。

【００６２】復号化鍵記憶部１１は、復号化鍵抽出部８によって抽出された復号化鍵を記憶するもので、上述したように記憶装置部４４に設けられる。

【００６３】秘匿情報消去部１２は、テレビ操作リモコン５０のデータ消去キー５４が押下されることによって、後述するように秘匿情報記憶部６から秘匿データを消去する。

【００６４】印刷処理部１３は、テレビ操作リモコン５０のデータ印刷キー５３が押下されることによって、後述するように秘匿データをプリンタ６０で印刷させるように処理して、赤外線送信部４６に出力する。

【００６５】制御部１４は、秘匿情報復号再生装置全体の処理を制御するものである。なお、必要に応じて、データ伝送エラーを訂正するエラー訂正部をシステムバス４に接続する。

【００６６】（秘匿データ受信記憶時の動作）第１の実施形態では、まず、テレビ放送局３０は、テレビ番組の開始時刻より前の時点において、そのテレビ番組と連動すべきデータを、秘匿データとして暗号化して、テレビ映像信号の垂直帰線消去期間を利用して放送する。

【００６７】この場合の暗号化方式としては、例えば、ＩＤＥＡ（Ｉｎｔｅｒｎａｔｉｏｎａｌ　Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ａｌｇｏｒｉｔｈｍ）を用いる。ＩＤＥＡは、スイス連邦工科大学において開発された暗号化方式であり、情報を暗号化するための暗号化鍵と、この暗号を解くための復号化鍵とが同一の鍵である共有鍵暗号方式（または秘密鍵暗号方式）である。鍵のビット長は１２８と定められている。ＩＤＥＡ暗号方式は、暗号メールソフトＰＧＰ（Ｐｒｅｔｔｙ　Ｇｏｏｄ　Ｐｒｉｖａｃｙ）にも使われており、鍵が１２８ビット長のＩＤＥＡは、現在主流のＤＥＳ（鍵は５６ビット長）、トリプルＤＥＳ（鍵は１１２ビット長）よりも、安全性が高いと言われている。

【００６８】なお、データを暗号化する暗号化方式としては、共有鍵暗号方式以外にも、公開鍵暗号方式、または公開鍵暗号方式と共有鍵暗号方式とを組み合わせたハイブリッド暗号方式を用いることができる。公開鍵暗号方式とは、暗号化鍵（公開鍵）と復号化鍵（秘密鍵）とが異なる場合の暗号化方式であり、ＲＳＡが代表的な方式である。公開鍵暗号方式を用いる場合には、テレビ放送局３０は、公開鍵で暗号化したデータを放送する。また、ハイブリッド暗号方式は、暗号化すべきデータごとにランダムなセッション鍵を作成して、そのセッション鍵でデータを暗号化し、次に、公開鍵暗号方式の公開鍵でセッション鍵を暗号化して、暗号化されたデータと暗号化されたセッション鍵とを一緒にして放送する方式である。

【００６９】さらに、この実施形態では、テレビ放送局３０は、放送する秘匿データに対して、当該秘匿データを参照するテレビ番組の放送番組識別情報を付加して放送する。この放送番組識別情報としては、例えば、Ｇコード（ＶＣＲ・ＰＬＵＳとも呼ばれる、米国ジェムスター社製のテレビ番組識別コード）を用いる。

【００７０】そして、第１の実施形態の秘匿情報復号再生装置では、以下のように、テレビ放送局３０によって放送された秘匿データが受信され、秘匿情報記憶部６に記憶される。

【００７１】すなわち、図３は、この場合のデータ処理部１５が行う受信記憶処理ルーチンを示し、その受信記憶処理ルーチン１００では、まずステップ１０１において、データ検出部５でデジタルデータを検出したか否かを判断する。

【００７２】この例では、そのデジタルデータは、ＭＩＭＥ（Ｍｕｔｌｐｕｒｐｏｓｅ　Ｉｎｔｅｒｎｅｔ　Ｍａｉｌ　Ｅｘｔｅｎｓｉｏｎｓ）構文で表現されたものである。図４は、そのＭＩＭＥ構文で表現されたデジタ

ルデータの一例を示し、１つのデジタルデータ中に複数のオブジェクトを格納するために、マルチパートタイプを利用しており、図４の例では、”－－－－－－－－－－－－２４２４Ｆ８０３４８８”によって、各オブジェクトが区切られている。

【００７３】このうちの１つめのオブジェクトは、”Ｃｏｎｔｅｎｔ－Ｔｙｐｅ：ｔｅｘｔ／ｃｏｎｔｒｏｌ”以下に記述された内容である。”Ｃｏｎｔｅｎｔ－Ｔｙｐｅ：ｔｅｘｔ／ｃｏｎｔｒｏｌ”以下の部分には、テレビ受信機４０が当該デジタルデータをどのように処理すべきかを記述するようになっており、図４の例では、当該デジタルデータを表示（または再生）すべきタイミングを記述している。

【００７４】”＜ｐｒｏｇｒａｍ　ｇｃｏｄｅ＝４２５３３４　ｉｄ＝３２＞”の部分が、その表示タイミングを記述した部分であり、当該デジタルデータを表示すべきテレビ番組の番組識別子と、このテレビ番組中でのデジタルデータのデータ識別子とが記述されている。すなわち、テレビ受信機４０が、Ｇコード番号が４２５３３４のテレビ番組を受信している最中に、デジタルデータ識別子が３２のデジタルデータの表示開始命令を受信した場合には、そのタイミングで当該デジタルデータをテレビ受信機４０に表示することとなる。

【００７５】なお、デジタルデータを表示すべきタイミングを示す情報は、絶対時刻、または番組開始時点からの相対時間でもよい。

【００７６】一方、２つめのオブジェクトは、”Ｃｏｎｔｅｎｔ－Ｔｙｐｅ：ａｐｐｌｉｃａｔｉｏｎ／ｅｎｃｒｉｐｔｅｄ－ｂｙ－ｉｄｅａ”以下に記述された内容である。”Ｃｏｎｔｅｎｔ－Ｔｙｐｅ：ａｐｐｌｉｃａｔｉｏｎ／ｅｎｃｒｉｐｔｅｄ－ｂｙ－ｉｄｅａ”以下の部分には、ＩＤＥＡ暗号方式で暗号化された秘匿データを記述するようになっている。ここで、”ａｐｐｌｉｃａｔｉｏｎ／ｅｎｃｒｉｐｔｅｄ－ｂｙ－ｉｄｅａ”という構文は、ＩＤＥＡ暗号を処理するアプリケーションを実行して、当該オブジェクトを処理すべきことを示す構文である。

【００７７】また、図４の例のように、”Ｃｏｎｔｅｎｔ－Ｔｒａｎｓｆｅｒ－Ｅｎｃｏｄｉｎｇ：ｂａｓｅ６４”の記述がある場合には、暗号化された秘匿データをさらにｂａｓｅ６４形式にエンコードして記述するようになっている。Ｂａｓｅ６４は、バイナリデータの８ビット×３バイトを６ビット×４バイトに振り分けて、それを通信データの７ビットに変換する方法である。

【００７８】なお、複数の情報を多重化する方法としては、ＭＩＭＥエンコードを用いる代わりに、ＭＰＥＧ－２Ｓｙｓｔｅｍｓに準拠したパケット多重方式を用いてもよい。ＭＰＥＧ－２Ｓｙｓｔｅｍｓでは、ＴＳ（Ｔｒａｎｓｐｏｒｔ　Ｓｔｒｅａｍ）パケットと呼ぶ１８８バイト固定長のパケットを伝送の基本単位としており、このＴＳパケットのパケットヘッダにパケット識別のためのＰＩＤ（Ｐａｃｋｅｔ　Ｉｄｅｎｔｉｆｉｅｒ）を含む構造となっている。

【００７９】データ検出部５が、デジタルデータとして上記のＭＩＭＥデータを検出したときには、ステップ１０２に進んで、データ検出部５は、その検出したＭＩＭＥデータをデコードする。

【００８０】受信記憶処理ルーチン１００では、次にステップ１０３において、そのデコードされたデータ、すなわち、ＭＩＭＥデータから抽出された秘匿データ、その秘匿データについての暗号化方式、およびその秘匿データを特定するための識別情報を、秘匿情報記憶部６に記憶する。

【００８１】図５は、秘匿情報記憶部６における記憶状態の一例を示す。同図に示すように、秘匿情報記憶部６は、秘匿データと、その秘匿データについての暗号化方式と、その秘匿データを特定するための識別情報であるＧコード（テレビ番組識別子）およびＩＤ（デジタルデータ識別子）とを、対応づけて記憶する。

【００８２】（秘匿データ復号再生時の動作）上述したように秘匿データを放送した後、テレビ放送局３０は、テレビ番組の進行に合わせて、秘匿データを復号化するための復号化鍵を放送する。第１の実施形態では、上述したように、復号化鍵もテレビ映像信号の垂直帰線消去期間を利用して放送する。

【００８３】そして、第１の実施形態の秘匿情報復号再生装置では、以下のように、テレビ放送局３０によって放送された復号化鍵が受信され、その復号化鍵によって秘匿情報記憶部６に記憶されている秘匿データが復号化されて、画像として表示される。

【００８４】すなわち、図６は、この場合のデータ処理部１５が行う復号再生処理ルーチンを示し、その復号再生処理ルーチン２００では、まずステップ２０１において、データ検出部５でデジタルデータを検出したか否かを判断する。

【００８５】この例では、そのデジタルデータも、ＭＩＭＥ構文で表現されたものである。図７は、そのＭＩＭＥ構文で表現されたデジタルデータの一例を示し、図４において上述したように、”Ｃｏｎｔｅｎｔ－Ｔｙｐｅ：ｔｅｘｔ／ｃｏｎｔｒｏｌ”以下の部分は、テレビ受信機４０が当該デジタルデータをどのように処理すべきかを記述している部分であり、図７の例では、添付した復号化鍵によって、秘匿情報記憶部６に記憶されている秘匿データを復号化し、再生するように指示している。

【００８６】”＜ｐｌａｙ　ｇｃｏｄｅ＝４２５３３４　ｉｄ＝３２　ｄｅｃｒｙｐｔｉｏｎ－ｋｅｙ－ｂａｓｅ６４＝ＧＴｖｂ７ｕｊＪｎ８５ｂＢＧ４ＶｆｙＦ７Ｇ１＝＝＞”という構文は、Ｇコード番号が４２５３３４であり、かつデジタルデータ識別子が３２である秘匿デ

ータが、秘匿情報記憶部６に記憶されているならば、復号化鍵”ＧＴｖｂ７ｕｊＪｎ８５ｂＢＧ４ＶｆｙＦ７Ｇ１＝＝”（１２８ｂｉｔ）を用いて、その秘匿データを復号化し、正常に復号化できた場合には、テレビ受信機４０に表示するように指示する命令文である。この例では、復号化鍵はｂａｓｅ６４によってエンコードされている。

【００８７】データ検出部５が、デジタルデータとして上記のＭＩＭＥデータを検出したときには、ステップ２０２に進んで、データ検出部５は、その検出したＭＩＭＥデータをデコードし、復号化鍵抽出部８は、そのデコードされたデータから復号化鍵を抽出する。

【００８８】次に、ステップ２０３において、秘匿情報特定部７は、そのデコードされたデータ、すなわちＭＩＭＥデータから抽出された情報中の、秘匿データ特定情報、図７の例では”ｇｃｏｄｅ＝４２５３３４　ｉｄ＝３２”という情報に基づいて、秘匿情報記憶部６に記憶されている秘匿データを検索して、テレビ番組と連動して復号化すべき秘匿データを特定できるか否かを判断する。

【００８９】例えば、テレビ番組の開始前の秘匿データの放送時に、視聴者がテレビ放送を受信していなかった場合には、秘匿情報記憶部６には、秘匿データ特定識別情報によって特定されるべき秘匿データが記憶されていないので、ステップ２０３では特定不能と判断されて、ステップ２０１に戻る。

【００９０】ステップ２０３で、秘匿情報特定部７が、テレビ番組と連動して復号化すべき秘匿データを特定できると判断したときには、ステップ２０４に進んで、秘匿情報特定部７は、テレビ番組と連動して復号化すべき秘匿データを特定する。

【００９１】さらに、ステップ２０５において、秘匿情報復号化部９は、その秘匿情報特定部７によって特定された、秘匿情報記憶部６に記憶されている秘匿データを、ステップ２０２で復号化鍵抽出部８によって抽出された復号化鍵、図７の例では復号化鍵”ＧＴｖｂ７ｕｊＪｎ８５ｂＢＧ４ＶｆｙＦ７Ｇ１＝＝”を用いて復号化する。この復号化の際には、秘匿情報記憶部６に記憶されている暗号化方式を用いる。

【００９２】復号再生処理ルーチン２００では、さらにステップ２０６において、復号化鍵抽出部８によって抽出された復号化鍵を、復号化鍵記憶部１１に記憶する。この場合、図８に一例を示すように、復号化鍵記憶部１１には、復号化鍵と、その復号化鍵の復号化鍵記憶部１１への記憶時刻と、その復号化鍵によって復号化された秘匿データの秘匿情報記憶部６における記憶位置（図５のＮｏカラムの値）ととを、対応づけて記憶する。

【００９３】そして、ステップ２０７において、ステップ２０５で秘匿情報復号化部９によって復号化されたデータを、秘匿情報再生部１０で処理して、映像・音声・データ出力部３に出力する。これによって、テレビ番組と連動して表示されるべき秘匿データが、図１に示したように、データ画像４３として、テレビ映像４２とともに表示される。

【００９４】復号再生処理ルーチン２００では示していないが、このようにテレビ受信機４０にデータ画像４３が表示されているタイミングで、視聴者がテレビ操作リモコン５０のデータ印刷キー５３を押下すると、そのとき表示されている秘匿データが、印刷処理部１３で印刷処理されて、赤外線送信部４６からプリンタ６０に送信され、プリンタ６０で画像として印刷される。

【００９５】（秘匿データの再表示と消去）第１の実施形態では、復号化鍵記憶部１１が設けられて、これに復号化鍵が記憶されるので、復号化鍵記憶部１１に復号化鍵が記憶された後においては、視聴者は、復号化鍵記憶部１１に記憶されている復号化鍵によって、いつでも、秘匿情報記憶部６に記憶されている秘匿データを復号化して、再表示することができる。

【００９６】秘匿データを再表示する場合には、視聴者は、テレビ操作リモコン５０のデータ選択ダイヤル５１を回して、秘匿情報記憶部６に記録されている秘匿データ、および復号化鍵記憶部１１に記憶されている復号化鍵を、次々と呼び出す。

【００９７】図８に示して上述したように、復号化鍵記憶部１１には、復号化鍵の復号化鍵記憶部１１への記憶時刻と、その復号化鍵によって復号化された秘匿データの秘匿情報記憶部６における記憶位置とが記憶されている。

【００９８】視聴者がデータ選択ダイヤル５１を左に回すと、データ処理部１５は、この復号化鍵記憶部１１に記憶されている記憶時刻から、復号化鍵記憶部１１に最も後に記憶された復号化鍵から順に復号化鍵を特定して、復号化鍵記憶部１１から呼び出すとともに、復号化鍵記憶部１１に記憶されている秘匿データ記憶位置から、その呼び出される復号化鍵によって復号化される秘匿データを、秘匿情報記憶部６から呼び出す。

【００９９】呼び出された秘匿データは、復号化鍵復号化部９において、呼び出された復号化鍵によって復号化され、その暗号化された秘匿データが、秘匿情報再生部１０で処理されて、映像・音声・データ出力部３に出力され、テレビ受信機４０に再表示される。

【０１００】逆にデータ選択ダイヤル５１を右に回すと、その時点で再表示されている秘匿データを復号化する復号化鍵より、より後に復号化鍵記憶部１１に記録された復号化鍵によって復号化される秘匿データが順次、復号化されて、テレビ受信機４０に再表示される。

【０１０１】このようにデータ選択ダイヤル５１の操作によって秘匿データを再表示した状態で、視聴者がテレビ操作リモコン５０のデータ印刷キー５３を押下すると、そのとき再表示されている秘匿データが、印刷処理

部１３で印刷処理されて、赤外線送信部４６からプリンタ６０に送信され、プリンタ６０で画像として印刷される。

【０１０２】上記の例のように、秘匿情報記憶部６に記憶される秘匿データがＨＴＭＬ書式のインターネットデータである場合には、データ中にリンク情報が埋め込まれている場合があるので、データ選択ダイヤル５１によってリンクアンカーを指定できるようにしてもよい。

【０１０３】この場合、指定されたリンクアンカーから辿ったリンク先のデータが、秘匿情報記憶部６に記憶された秘匿データであった場合には、この秘匿データの秘匿情報記憶部６における記憶位置（図５のＮｏカラムの値）を検索キーとして、図８に示した復号化鍵記憶部１１における秘匿データアドレスカラムを検索して、対応する復号化鍵を特定する。そして、この秘匿データを復号化して、テレビ受信機４０に再表示するようにする。

【０１０４】秘匿情報記憶部６に記憶された秘匿データ中には、テレビ番組放送時に参照される（復号化される）情報もあれば、参照されない（復号化されない）情報もある。しかし、いづれの情報であっても、テレビ番組終了時には消去するようにしても構わない。

【０１０５】秘匿情報記憶部６に記憶されている秘匿データをテレビ番組終了時に消去するには、例えば、視聴者が適当な時点でテレビ操作リモコン５０のデータ消去キー５４を押下することによって、秘匿情報消去部１２が、図５に示したように秘匿情報記憶部６に記憶されているＧコードに含まれる放送時刻情報から、番組終了時刻を検出して、番組終了時刻を過ぎた秘匿データのみを、秘匿情報記憶部６から消去するようにする。または、放送局が、番組終了時に番組終了を通知する信号を放送し、テレビ受信機４０では、この信号を検知して、秘匿情報消去部１２が、番組終了時刻を過ぎた秘匿データのみを、秘匿情報記憶部６から消去するようにしてもよい。

【０１０６】（変形例）秘匿データは、複数の特定の復号化鍵を組み合わせた場合にのみ正しく復号化できるものとすることもできる。この場合には、その秘匿データが秘匿情報記憶部６に記憶されている状態で、放送局からテレビ番組と連動して順次、送信された複数の復号化鍵を順次、復号化鍵記憶部１１に記憶し、秘匿データを復号化するための復号化鍵が揃った時点で、秘匿データを復号化するようにする。このようにすることによって、例えば、１０回に渡って連続するドラマの１０回すべてを視聴した視聴者にだけ、放送局から有益な情報を提供するというようなことができる。

【０１０７】地上波テレビ放送の放送電波によって秘匿データまたは復号化鍵を伝送する方法としては、テレビ映像信号の垂直帰線消去期間を利用する以外に、音声副搬送波を利用することもできる。音声副搬送波を用いてデータを放送する場合には、音声信号の空いている２チャンネル分の周波数を使ってデータを送る。１チャンネル当たり約９．６ｋｂｐｓの伝送容量があるので、２チャンネル分では約１９．２ｋｂｐｓのインターネットデータを放送することができる。

【０１０８】また、上記の例は、復号化鍵をテレビ映像情報およびテレビ音声情報に対して独立した情報として送信する場合であるが、データハイディング技術（日経エレクトロニクス、Ｎｏ．６８３，ｐｐ１４９－１６２，１９９７．２．２４）を用いて、復号化鍵をテレビ映像情報またはテレビ音声情報に埋め込んで放送してもよい。この場合には、復号化鍵抽出部８を、アナログ復調部２からの映像情報または音声情報から復号化鍵を抽出して、システムバス４に出力するものとする。

【０１０９】このように、テレビ映像情報またはテレビ音声情報に復号化鍵を埋め込んで放送する場合には、ビデオ録画した後でも、録画されたテレビ映像情報またはテレビ音声情報の中に復号化鍵を保持できるので、ビデオ映像を再生表示しながら、ビデオ映像に関連した秘匿情報を復号化して表示できるようになる。

【０１１０】また、上記の例は、放送局が秘匿データを放送する場合であるが、秘匿データを視聴者に配信する方法としては、放送局などが秘匿データをＣＤＲＯＭなどの記憶媒体に記憶させて、この記憶媒体そのものを視聴者に配布するようにしてもよい。この場合には、その記録媒体が秘匿情報記憶部６を構成することになる。

【０１１１】さらに、上述した第１の実施形態は、デジタルテレビ放送の送受信システムにも適用することができる。例えば、人工衛星を利用した衛星デジタルテレビ放送でも、デジタル化したテレビ映像情報およびテレビ音声情報にＨＴＭＬ書式のインターネットデータを多重化して放送する試みが開始されており、この衛星データ放送を受信する場合には、約１．５Ｍｂｐｓで高速伝送されるインターネットデータを受信することができる。

【０１１２】（効果）上述した第１の実施形態によれば、テレビ番組を視聴した人だけが知ることができる秘匿情報をテレビ番組の放送に先立って予め配信することができ、秘匿情報を不特定多数の視聴者に対して配信する場合でも、テレビ番組を見た視聴者だけに情報を知る権利を与えることができる。

【０１１３】また、テレビ番組の進行に合わせて、情報の公開・非公開を動的に変更することができるとともに、同一の秘匿情報を複数の場面または番組で利用する場合には、一度配信した秘匿情報を再利用することができる。

【０１１４】さらに、視聴者が秘匿情報を復号化する操作を強いられず、視聴しているテレビ番組に集中できるようになる。また、ＣＤＲＯＭなどの放送以外のメディアによって視聴者に提供された秘匿情報でも、テレビ番組に連動させて復号化して再生することができる。

【０１１５】［第２の実施形態］第１の実施形態は、放

送局が、不特定多数の視聴者に対して、暗号化されたＷｅｂページを予め配信しておき、テレビ番組を見た視聴者だけが、その秘匿Ｗｅｂページの内容を見ることができるようにした場合である。

【０１１６】これに対して、第２の実施形態は、情報提供者が許可した特定の視聴者だけにアクセスを許すＷｅｂページを放送する場合である。すなわち、第２の実施形態では、放送局は、秘匿Ｗｅｂページをテレビ番組の開始に先立って放送し、放送局（情報提供者）が許可した視聴者だけが、テレビ番組の進行に合わせて、その秘匿Ｗｅｂページを読み出して見ることができるようにする。

【０１１７】また、第２の実施形態は、この発明を衛星デジタルテレビ放送の送受信システムに適用した場合である。この衛星デジタルテレビ放送を受信する受信機は、例えば、日本国内で放送が開始されているＰｅｒｆｅｃＴＶ！放送を受信する受信機である。

【０１１８】（構成）第２の実施形態では、テレビ受信機にはＩＣカードを装着できるようにする。図１０に示すように、このＩＣカード８１内には、メモリ部８２のほかに演算部８３を設け、メモリ部８２には、ユーザＩＤ、およびユーザ鍵Ｋｕを記憶させる。演算部８３は、後述するように鍵復号化演算を行うものである。

【０１１９】ユーザ鍵Ｋｕは、視聴者が放送によって配信された秘匿データを復号化する権利を有するか否かを識別するために用いられる鍵であって、各視聴者ごとに異なるものである。なお、衛星デジタルテレビ放送などの、映像スクランブルの復号に用いられている、視聴者ごとに異なる復号化鍵を、この実施形態のユーザ鍵Ｋｕとして用いてもよい。

【０１２０】第２の実施形態では、放送局は、図９に示すように、放送局データベース７１として、放送データを管理するための放送データ管理データベース７２と、ユーザ情報を管理するためのユーザ管理データベース７３とを備え、放送データ管理データベース７２には、放送データ、暗号化／復号化鍵Ｋｅ、および秘匿データ特定情報を保持し、ユーザ管理データベース７３には、宛先ユーザＩＤ、および宛先ユーザのユーザ鍵Ｋｕを保持するものとする。

【０１２１】放送データ管理データベース７２の放送データは、暗号化して秘匿データとするデータである。

【０１２２】鍵Ｋｅは、その放送データを暗号化するための暗号化鍵であり、かつ、この鍵Ｋｅによって暗号化された秘匿データを復号化するための復号化鍵である。すなわち、第２の実施形態では、情報を暗号化するための暗号化鍵と、この暗号を解くための復号化鍵とが同一の鍵である共有鍵暗号方式を用いる。

【０１２３】ただし、データを暗号化する暗号化方式としては、共有鍵暗号方式以外にも、公開鍵暗号方式、または公開鍵暗号方式と共有鍵暗号方式とを組み合わせたハイブリッド暗号方式を用いてもよい。例えば、公開鍵暗号方式を用いる場合には、暗号化鍵Ｋｅと復号化鍵Ｋｅとは、公開鍵ペアとなるように生成する。

【０１２４】放送データ管理データベース７２の秘匿データ特定情報は、秘匿データを特定するための識別情報であり、例えば、放送番組識別子としてのＧコード、およびデジタルデータ識別子である。

【０１２５】ユーザ管理データベース７３のユーザ鍵Ｋｕは、上記の鍵Ｋｅを暗号化する鍵である。すなわち、放送局のユーザ管理データベース７３には、各視聴者が保持するＩＣカード８１に記憶されているユーザ鍵（第２の復号化鍵）Ｋｕと同一のユーザ鍵（第２の暗号化鍵）Ｋｕが保持される。したがって、ユーザ管理データベース７３に保持されるユーザ鍵Ｋｕで暗号化された復号化鍵Ｋｅは、視聴者が保持するＩＣカード８１に記憶されているユーザ鍵Ｋｕで復号化することによって、取り出せることになる。

【０１２６】なお、この場合も、公開鍵暗号方式、または公開鍵暗号方式と共有鍵暗号方式とを組み合わせたハイブリッド暗号方式を用いてもよい。例えば、ユーザ管理データベース７３に保持されるユーザ鍵Ｋｕと、各視聴者が保持するＩＣカード８１に記憶されているユーザ鍵Ｋｕとを、公開鍵ペアとなるように生成する。

【０１２７】（秘匿データ受信記憶時の動作）テレビ番組の開始に先立って、放送局は秘匿データを放送し、テレビ受信機は、その放送された秘匿データを受信して秘匿情報記憶部に記憶する。

【０１２８】具体的に、図１１に示すように、テレビ放送局７０では、暗号化すべき放送データごとにランダムな暗号化鍵Ｋｅを作成して、データ暗号化部７４において、その暗号化鍵Ｋｅで放送データを暗号化し、その暗号化された秘匿データを、テレビ番組の開始時刻より前の時点において放送する。

【０１２９】この場合、ＭＩＭＥエンコーダ７５において、その暗号化された秘匿データに対して、この秘匿データを受信すべき視聴者を指定する宛先ユーザＩＤリストと、この秘匿データを後から特定できるようにするための秘匿データ特定情報、例えば上記のＧコードおよびデジタルデータ識別子とを、多重化して放送する。

【０１３０】図１２に示すように、テレビ受信機４０では、ＭＩＭＥデコーダ２１によって、テレビ放送局７０からの多重化された放送信号から、暗号化された秘匿データ、宛先ユーザＩＤリスト、および秘匿データ特定情報を分離し、宛先照合部２２において、宛先ユーザＩＤリスト中に、ＩＣカード８１に記憶されている自分のユーザＩＤが含まれているか否かを照合する。

【０１３１】そして、宛先ユーザＩＤリスト中に自分のユーザＩＤが含まれている場合には、受信した秘匿データおよび秘匿データ特定情報を自分宛てのものとして、その秘匿データおよび秘匿データ特定情報を秘匿情報記

憶部６に記憶する。この場合、秘匿情報記憶部６は、図５に示したように、秘匿データ、その秘匿データについての暗号化方式、および秘匿データ特定情報を、対応づけて記憶する。

【０１３２】（秘匿データ復号再生時の動作）放送局は、テレビ番組と連動して復号化されるべき秘匿データを復号化するための復号化鍵Ｋｅを、その秘匿データを正しく復号化する権利を有する視聴者のユーザ鍵Ｋｕによって暗号化して、テレビ番組の進行に合わせて放送する。

【０１３３】すなわち、図１３に示すように、テレビ放送局７０では、鍵暗号化部７６において、復号化鍵Ｋｅ（秘匿データを暗号化したときの暗号化鍵Ｋｅと同一の鍵）を、宛先視聴者に固有のユーザ鍵Ｋｕ（宛先視聴者のＩＣカード８１内のユーザ鍵Ｋｕと同一の鍵）によって、宛先視聴者の数だけ暗号化し、その暗号化された復号化鍵Ｋｅ´のリストを、テレビ番組の進行に合わせて放送する。

【０１３４】この場合、ＭＩＭＥエンコーダ７５において、その暗号化された復号化鍵Ｋｅ´のリストに対して、この復号化鍵Ｋｅ´の宛先視聴者を指定する宛先ユーザＩＤリストと、この復号化鍵Ｋｅ´によって復号化されるべき秘匿データを特定するための秘匿データ特定情報、例えば上記のＧコードおよびデジタルデータ識別子とを、多重化して放送する。

【０１３５】図１４に示すように、テレビ受信機４０では、ＭＩＭＥデコーダ２１によって、テレビ放送局７０からの多重化された放送信号から、暗号化された復号化鍵Ｋｅ´のリスト、宛先ユーザＩＤリスト、および秘匿データ特定情報を分離し、宛先照合部２２において、宛先ユーザＩＤリスト中に、ＩＣカード８１のメモリ部８２に記憶されている自分のユーザＩＤが含まれているか否かを照合する。

【０１３６】そして、宛先ユーザＩＤリスト中に自分のユーザＩＤが含まれている場合には、受信した暗号化された復号化鍵Ｋｅ´および秘匿データ特定情報を自分宛てのものとして、ＩＣカード８１内の演算部８３において、その暗号化された復号化鍵Ｋｅ´を、自分がＩＣカード８１のメモリ部８２内に所有する、自分に固有のユーザ鍵Ｋｕによって復号化して、復号化鍵Ｋｅを取り出す。

【０１３７】同時に、宛先ユーザＩＤリスト中に自分のユーザＩＤが含まれている場合には、秘匿情報特定部７は、秘匿情報記憶部６に記憶されている秘匿データのうちの、ＭＩＭＥデコーダ２１により分離された秘匿データ特定情報によって特定される秘匿データを特定し、さらに秘匿情報復号化部９は、その秘匿情報特定部７によって特定されて秘匿情報記憶部６から読み出された秘匿データを、ＩＣカード８１内の演算部８３から得られた復号化鍵Ｋｅによって復号化する。

【０１３８】その復号化された秘匿データは、秘匿情報再生部１０によって処理されて、映像・音声・データ出力部３に出力され、テレビ受信機４０の表示画面に表示される。

【０１３９】（効果）この第２の実施形態によれば、視聴者が不正に他人宛ての秘匿データを受信できるようにテレビ受信機４０を改造した場合でも、テレビ放送局７０が復号化鍵Ｋｅの暗号化の際に用いたユーザ鍵Ｋｕと、視聴者のＩＣカード８１に記憶されているユーザ鍵Ｋｕとが一致しない場合には、秘匿データを正しく復号化することができないので、システムの安全性が保証される。

【０１４０】［第３の実施形態］第２の実施形態は、情報提供者が許可した特定の視聴者だけにアクセスを許すＷｅｂページを放送する場合に、すでに放送した秘匿Ｗｅｂページを復号化するための復号化鍵Ｋｅを、宛先視聴者に固有のユーザ鍵Ｋｕによって、宛先視聴者の数だけ暗号化して、放送するもので、放送局の放送システムおよび受信側の受信システムを比較的簡単にできる特長があるが、テレビ番組と同期したタイミングで、宛先視聴者ごとに異なる暗号化された復号化鍵Ｋｅ´を放送するため、宛先視聴者の数が多い場合には、テレビ番組の進行に合わせて復号化鍵を送信することが困難になる可能性がある。

【０１４１】そこで、第３の実施形態は、テレビ番組の開始に先立って秘匿データを放送する際に、当該秘匿データを復号化するための復号化鍵を暗号化して、秘匿データとともに放送し、その後、テレビ番組の進行に合わせて、先に放送した暗号化された復号化鍵を復号化するための復号化鍵を放送し、これによって得られた復号化鍵を用いて当該秘匿データを復号化するものである。

【０１４２】この場合、秘匿データとともに放送する暗号化された復号化鍵は、各視聴者ごとに異なる個別復号化鍵とし、テレビ番組の進行に合わせて放送する復号化鍵は、全視聴者に共通の共通復号化鍵とする。

【０１４３】この第３の実施形態によれば、秘匿データを復号化するための復号化鍵の宛先が多い場合でも、テレビ番組の進行に合わせて放送する復号化鍵は、わずかに１つで済むので、テレビ番組の進行に合わせて復号化鍵を送信することが困難になるというようなことは全くない。

【０１４４】第３の実施形態も、第２の実施形態と同様に、この発明を衛星デジタルテレビ放送の送受信システムに適用した場合である。この衛星デジタルテレビ放送を受信する受信機は、例えば、日本国内で放送が開始されているＰｅｒｆｅｃＴＶ！放送を受信する受信機である。

【０１４５】（構成）第３の実施形態でも、第２の実施形態と同様に、テレビ受信機にはＩＣカードを装着できるようにする。第２の実施形態と同様に、図１０に示す

ように、このＩＣカード８１のメモリ部８２には、ユーザ鍵Ｋｕを記憶させる。第２の実施形態と同様に、このユーザ鍵Ｋｕは、視聴者が放送によって配信された秘匿データを復号化する権利を有するか否かを識別するために用いられる鍵であって、各視聴者ごとに異なるものである。

【０１４６】第２の実施形態と同様に、ＩＣカード８１は内部に演算部８３を備えるものとする。また、第３の実施形態では、図１７に示すように、テレビ受信機４０は、さらに暗号化鍵記憶部２３を備えるものとする。

【０１４７】放送局データベース７１については、第３の実施形態では、図１５に示すように、放送データ管理データベース７２には、上述した第１の暗号化鍵としての暗号化／復号化鍵Ｋｅとともに、第３の暗号化鍵としての暗号化／復号化鍵Ｋｃを保持するようにする。ユーザ管理データベース７３には、第２の暗号化鍵としてのユーザ鍵Ｋｕを保持することは、第２の実施形態と同じである。

【０１４８】第３の暗号化鍵としての暗号化／復号化鍵Ｋｃは、テレビ番組の進行に合わせて放送する鍵であって、全視聴者に共通のものである。

【０１４９】（秘匿データ受信記憶時の動作）テレビ番組の開始に先立って、放送局は、上記の第１暗号化鍵Ｋｅを第２暗号化鍵Ｋｕで暗号化し、その暗号化された暗号化鍵Ｋｅ′を、さらに第３暗号化鍵Ｋｃで暗号化して、その暗号化された暗号化鍵Ｋｅ″と、秘匿データとを放送し、テレビ受信機は、その放送された秘匿データおよび暗号化された暗号化鍵Ｋｅ″を受信して、秘匿データを秘匿情報記憶部に記憶し、暗号化された暗号化鍵Ｋｅ″を上記の暗号化鍵記憶部に記憶する。

【０１５０】すなわち、図１６に示すように、テレビ放送局７０では、暗号化すべき放送データごとにランダムな第１暗号化鍵Ｋｅおよび第３暗号化鍵Ｋｃを作成して、データ暗号化部７４において、その第１暗号化鍵Ｋｅで放送データを暗号化し、その暗号化された秘匿データを、ＭＩＭＥエンコーダ７５に送出する。

【０１５１】また、鍵暗号化部７６において、第１復号化鍵Ｋｅを、宛先視聴者に固有の第２暗号化鍵（ユーザ鍵）Ｋｕによって、宛先視聴者の数だけ暗号化して、その暗号化された暗号化鍵Ｋｅ′のリストを得る。さらに、鍵暗号化部７７において、その暗号化された暗号化鍵Ｋｅ′のリストを、第３暗号化鍵Ｋｃで暗号化して、その暗号化された暗号化鍵Ｋｅ″のリストを、ＭＩＭＥエンコーダ７５に送出する。

【０１５２】そして、ＭＩＭＥエンコーダ７５において、暗号化された秘匿データ、暗号化された暗号化鍵Ｋｅ″のリスト、宛先ユーザＩＤリスト、および秘匿データ特定情報を多重化して、テレビ番組の開始時刻より前の時点において放送する。

【０１５３】図１７に示すように、テレビ受信機４０では、ＭＩＭＥデコーダ２１によって、テレビ放送局７０からの多重化された放送信号から、暗号化された秘匿データ、暗号化された暗号化鍵Ｋｅ″のリスト、宛先ユーザＩＤリスト、および秘匿データ特定情報を分離し、宛先照合部２２において、宛先ユーザＩＤリスト中に、ＩＣカード８１に記憶されている自分のユーザＩＤが含まれているか否かを照合する。

【０１５４】そして、宛先ユーザＩＤリスト中に自分のユーザＩＤが含まれている場合には、受信した秘匿データおよび暗号化された暗号化鍵Ｋｅ″などを自分宛てのものとして、その秘匿データおよび秘匿データ特定情報を秘匿情報記憶部６に記憶するとともに、暗号化された暗号化鍵Ｋｅ″を暗号化鍵記憶部２３に記憶する。

【０１５５】この場合、秘匿情報記憶部６は、図５に示したように、秘匿データ、その秘匿データについての暗号化方式、および秘匿データ特定情報を、対応づけて記憶するとともに、記憶された秘匿データの秘匿情報記憶部６における記憶位置（図５のＮｏカラムの値）を、暗号化鍵記憶部２３に出力し、暗号化鍵記憶部２３は、図１８に示すように、暗号化された暗号化鍵Ｋｅ″と、秘匿情報記憶部６から入力された、秘匿データの秘匿情報記憶部６における記憶位置とを、対応づけて記憶する。

【０１５６】（秘匿データ復号再生時の動作）放送局は、上記の第３暗号化鍵Ｋｃを、テレビ番組と連動して復号化されるべき秘匿データを復号化するための復号化鍵として、テレビ番組の進行に合わせて放送する。

【０１５７】すなわち、図１９に示すように、テレビ放送局７０では、ＭＩＭＥエンコーダ７５において、復号化鍵（第３暗号化鍵）Ｋｃと、この復号化鍵Ｋｃによって復号化されるべき秘匿データを特定するための秘匿データ特定情報とを、多重化して、テレビ番組の進行に合わせて放送する。

【０１５８】図２０に示すように、テレビ受信機４０では、ＭＩＭＥデコーダ２１によって、テレビ放送局７０からの多重化された放送信号から、復号化鍵Ｋｃ、および秘匿データ特定情報を分離する。そして、秘匿情報特定部７は、秘匿情報記憶部６に記憶されている秘匿データのうちの、ＭＩＭＥデコーダ２１により分離された秘匿データ特定情報によって特定される秘匿データを特定して、その特定した秘匿データの秘匿情報記憶部６における記憶位置を、秘匿情報記憶部６から暗号化鍵記憶部２３に出力させる。

【０１５９】これによって、図１８に示したように秘匿データの秘匿情報記憶部６における記憶位置に対応して暗号化鍵記憶部２３に記憶されている、暗号化された暗号化鍵Ｋｅ″が、暗号化鍵記憶部２３から鍵復号化部２４に出力され、鍵復号化部２４において、暗号化された暗号化鍵Ｋｅ″が、ＭＩＭＥデコーダ２１により分離された復号化鍵Ｋｃによって復号化されて、鍵復号化部２４から、暗号化された暗号化鍵Ｋｅ′が出力される。

【０１６０】さらに、ＩＣカード８１内の演算部８３において、その暗号化された暗号化鍵Ｋｅ′が、ＩＣカード８１のメモリ部８２に記憶されているユーザ鍵Ｋｕによって復号化されて、演算部８３から、復号化鍵（第１暗号化鍵）Ｋｅが得られる。

【０１６１】そして、秘匿情報復号化部９において、秘匿情報特定部７によって特定されて秘匿情報記憶部６から読み出された秘匿データが、演算部８３から得られた復号化鍵Ｋｅによって復号化される。その復号化された秘匿データは、秘匿情報再生部１０によって処理されて、映像・音声・データ出力部３に出力され、テレビ受信機４０の表示画面に表示される。

【０１６２】（効果）この第３の実施形態によれば、第２の実施形態と同様に、視聴者が不正に他人宛ての秘匿データを受信できるようにテレビ受信機４０を改造した場合でも、テレビ放送局７０が復号化鍵Ｋｅの暗号化の際に用いたユーザ鍵Ｋｕと、視聴者のＩＣカード８１に記憶されているユーザ鍵Ｋｕとが一致しない場合には、秘匿データを正しく復号化することができないので、システムの安全性が保証される。

【０１６３】さらに、秘匿データを復号化するための復号化鍵の宛先が多い場合でも、テレビ番組の進行に合わせて放送する復号化鍵は、わずかに１つで済むので、テレビ番組の進行に合わせて復号化鍵を送信することが困難になるというようなことは全くない。

【０１６４】［第４の実施形態］第４の実施形態は、第３の実施形態の変形である。図１６に示したように、第３の実施形態では、放送局は、放送データを暗号化した第１暗号化鍵Ｋｅを、宛先視聴者に固有の第２暗号化鍵（ユーザ鍵）Ｋｕで、宛先視聴者の数だけ暗号化し、その後、さらに全視聴者に共通の第３暗号化鍵Ｋｃで暗号化する場合である。

【０１６５】これに対して、第４の実施形態では、放送局は、放送データを暗号化した第１暗号化鍵Ｋｅを、全視聴者に共通の第３暗号化鍵Ｋｃで暗号化した後に、宛先視聴者に固有の第２暗号化鍵（ユーザ鍵）Ｋｕで、宛先視聴者の数だけ暗号化する。

【０１６６】これによって、放送局の暗号化処理時間を短縮することができる。さらに、この第４の実施形態によれば、テレビ受信機がテレビ番組の進行に合わせてデータを復号化する際に、ＩＣカードにアクセスする必要がなくなるという効果がある。

【０１６７】（秘匿データ受信記憶時の動作）テレビ番組の開始に先立って、放送局は、上記の第１暗号化鍵Ｋｅを第３暗号化鍵Ｋｃで暗号化し、その暗号化された暗号化鍵Ｋｅ′を、さらに第２暗号化鍵Ｋｕで暗号化して、その暗号化された暗号化鍵Ｋｅ″と、秘匿データとを放送する。

【０１６８】すなわち、図２１に示すように、テレビ放送局７０では、暗号化すべき放送データごとにランダムな第１暗号化鍵Ｋｅおよび第３暗号化鍵Ｋｃを作成して、データ暗号化部７４において、その第１暗号化鍵Ｋｅで放送データを暗号化し、その暗号化された秘匿データを、ＭＩＭＥエンコーダ７５に送出する。

【０１６９】また、鍵暗号化部７６において、第１復号化鍵Ｋｅを、全視聴者に共通の第３暗号化鍵Ｋｃによって暗号化して、その暗号化された暗号化鍵Ｋｅ′を得る。さらに、鍵暗号化部７７において、その暗号化された暗号化鍵Ｋｅ′を、宛先視聴者に固有の第２暗号化鍵（ユーザ鍵）Ｋｕによって、宛先視聴者の数だけ暗号化して、その暗号化された暗号化鍵Ｋｅ″のリストを、ＭＩＭＥエンコーダ７５に送出する。

【０１７０】そして、ＭＩＭＥエンコーダ７５において、暗号化された秘匿データ、暗号化された暗号化鍵Ｋｅ″のリスト、宛先ユーザＩＤリスト、および秘匿データ特定情報を多重化して、テレビ番組の開始時刻より前の時点において放送する。

【０１７１】図２２に示すように、テレビ受信機４０では、ＭＩＭＥデコーダ２１によって、テレビ放送局７０からの多重化された放送信号から、暗号化された秘匿データ、暗号化された暗号化鍵Ｋｅ″のリスト、宛先ユーザＩＤリスト、および秘匿データ特定情報を分離し、宛先照合部２２において、宛先ユーザＩＤリスト中に、ＩＣカード８１に記憶されている自分のユーザＩＤが含まれているか否かを照合する。

【０１７２】そして、宛先ユーザＩＤリスト中に自分のユーザＩＤが含まれている場合には、受信した秘匿データおよび暗号化された暗号化鍵Ｋｅ″などを自分宛てのものとして、ＩＣカード８１内の演算部８３において、その暗号化された暗号化鍵Ｋｅ″を、自分がＩＣカード８１のメモリ部８２内に所有する、自分に固有のユーザ鍵Ｋｕによって復号化して、暗号化された暗号化鍵Ｋｅ′を取り出す。

【０１７３】そして、ＭＩＭＥデコーダ２１により分離された秘匿データおよび秘匿データ特定情報を秘匿情報記憶部６に記憶するとともに、演算部８３から得られた、暗号化された暗号化鍵Ｋｅ′を暗号化鍵記憶部２３に記憶する。

【０１７４】この場合、秘匿情報記憶部６は、図５に示したように、秘匿データ、その秘匿データについての暗号化方式、および秘匿データ特定情報を、対応づけて記憶するとともに、記憶された秘匿データの秘匿情報記憶部６における記憶位置（図５のＮｏカラムの値）を、暗号化鍵記憶部２３に出力し、暗号化鍵記憶部２３は、図２３に示すように、暗号化された暗号化鍵Ｋｅ′と、秘匿情報記憶部６から入力された、秘匿データの秘匿情報記憶部６における記憶位置とを、対応づけて記憶する。

【０１７５】（秘匿データ復号再生時の動作）放送局は、上記の第３暗号化鍵Ｋｃを、テレビ番組と連動して復号化されるべき秘匿データを復号化するための復号化

鍵として、テレビ番組の進行に合わせて放送する。

【０１７６】すなわち、図２４に示すように、テレビ放送局７０では、ＭＩＭＥエンコーダ７５において、復号化鍵（第３暗号化鍵）Ｋｃと、この復号化鍵Ｋｃによって復号化されるべき秘匿データを特定するための秘匿データ特定情報とを、多重化して、テレビ番組の進行に合わせて放送する。

【０１７７】図２５に示すように、テレビ受信機４０では、ＭＩＭＥデコーダ２１によって、テレビ放送局７０からの多重化された放送信号から、復号化鍵Ｋｃ、および秘匿データ特定情報を分離する。そして、秘匿情報特定部７は、秘匿情報記憶部６に記憶されている秘匿データのうちの、ＭＩＭＥデコーダ２１により分離された秘匿データ特定情報によって特定される秘匿データを特定して、その特定した秘匿データの秘匿情報記憶部６における記憶位置を、秘匿情報記憶部６から暗号化鍵記憶部２３に出力させる。

【０１７８】これによって、図２３に示したように秘匿データの秘匿情報記憶部６における記憶位置に対応して暗号化鍵記憶部２３に記憶されている、暗号化された暗号化鍵Ｋｅ´が、暗号化鍵記憶部２３から鍵復号化部２４に出力され、鍵復号化部２４において、暗号化された暗号化鍵Ｋｅ´が、ＭＩＭＥデコーダ２１により分離された復号化鍵Ｋｃによって復号化されて、鍵復号化部２４から、復号化鍵（第１暗号化鍵）Ｋｅが出力される。

【０１７９】そして、秘匿情報復号化部９において、秘匿情報特定部７によって特定されて秘匿情報記憶部６から読み出された秘匿データが、鍵復号化部２４から得られた復号化鍵Ｋｅによって復号化される。その復号化された秘匿データは、秘匿情報再生部１０によって処理されて、映像・音声・データ出力部３に出力され、テレビ受信機４０の表示画面に表示される。

【０１８０】（効果）この第４の実施形態によれば、第２または第３の実施形態と同様に、視聴者が不正に他人宛ての秘匿データを受信できるようにテレビ受信機４０を改造した場合でも、テレビ放送局７０が復号化鍵Ｋｅの暗号化の際に用いたユーザ鍵Ｋｕと、視聴者のＩＣカード８１に記憶されているユーザ鍵Ｋｕとが一致しない場合には、秘匿データを正しく復号化することができないので、システムの安全性が保証される。

【０１８１】また、第３の実施形態と同様に、秘匿データを復号化するための復号化鍵の宛先が多い場合でも、テレビ番組の進行に合わせて放送する復号化鍵は、わずかに１つで済むので、テレビ番組の進行に合わせて復号化鍵を送信することが困難になるというようなことは全くない。

【０１８２】さらに、テレビ受信機４０がテレビ番組の進行に合わせてデータを復号化する際に、ＩＣカード８１にアクセスする必要がなくなる。

【０１８３】〔その他の実施形態〕上述した各実施形態は、この発明をテレビ放送の送受信システムに適用した場合であるが、この発明はラジオ放送の送受信システムにも適用することができる。

【０１８４】秘匿情報、またはテレビ放送信号またはラジオ放送信号に重畳されるデータとしては、電波またはケーブルによって伝送されたテレビ放送信号の垂直帰線消去期間に多重化された情報、テレビ放送またはラジオ放送の音声副チャンネルによって伝送された情報、テレビ放送またはラジオ放送の音声副搬送波によって伝送された情報、デジタルテレビ放送に複合化された情報、またはテレビ放送またはラジオ放送の映像情報または音声情報に埋め込まれた隠し情報が考えられるが、この発明は、これらのいずれの場合にも適用することができる。

【０１８５】［各種の実施形態と効果］この発明では、以下のような実施形態にすることによって、それぞれ以下のような効果が得られる。

【０１８６】（１）放送局は、秘匿データを復号化するための復号化鍵と、この復号化鍵を適用すべき秘匿データを特定する秘匿データ特定情報とを、テレビ映像番組の進行に合わせて放送し、テレビ受信機は、放送された復号化鍵と秘匿データ特定情報とを受信して、記憶媒体に記憶された秘匿データのうちの、秘匿データ特定情報によって特定された秘匿データを、復号化鍵によって復号化するように構成することにより、不特定多数人に対してデータを予め配信しておいた場合でも、テレビ番組を見た視聴者だけが、このデータの内容を見ることができるようになり、これによって、放送局は、テレビ番組を見た視聴者だけに有益なデータを提供することができる。

【０１８７】（２）テレビ受信機によって、放送された復号化鍵と秘匿データ特定情報とを受信し、記憶媒体に記憶された秘匿データのうちの、秘匿データ特定情報によって特定された秘匿データを、復号化鍵によって復号化し、この復号化されたデータをテレビ映像番組の進行に合わせてテレビ受像機に表示再生するように構成することにより、テレビ番組を見た視聴者が、このデータの内容を見る場合でも、秘匿データを復号化する操作を強いられず、視聴しているテレビ番組に集中することができる。

【０１８８】（３）放送局によって放送された復号化鍵を記憶できるように構成することにより、視聴者は、復号化鍵が記憶された後のタイミングにおいて、秘匿データを随時復号化して表示再生することができる。

【０１８９】（４）放送局が、秘匿データを復号化するための復号化鍵とともに、放送番組識別情報をデータ放送した場合に、テレビ受信機によって、この放送された放送番組識別情報を受信し、記憶媒体に記憶された秘匿データのうちの、放送番組識別情報によって特定されたテレビ番組に関連する秘匿データを復号化鍵によって復号化するように構成することにより、不特定多数の視聴

者に対してテレビ番組に関連するデータを予め配信しておいた場合でも、テレビ番組を見た視聴者だけが、このデータの内容を見ることができるようになり、これによって、放送局は、テレビ番組を見た視聴者だけに有益なデータを提供することができる。

【０１９０】（５）テレビ受信機によって、放送局から放送された復号化鍵を受信した場合に、記憶媒体に記憶された秘匿データのうちの、視聴中のテレビチャンネル番号と復号化鍵受信時刻とに基づいて、記憶媒体に記憶された秘匿データのうちの、受信した復号化鍵に対応する秘匿データを特定するように構成することにより、放送局から放送番組識別情報が放送されなかった場合でも、放送中のテレビ番組に関連する秘匿データを特定することができるので、テレビ番組を見た視聴者だけが秘匿データの内容を見ることができるようになり、これによって、放送局は、テレビ番組を見た視聴者だけに有益なデータを提供することができる。

【０１９１】（６）秘匿データを、放送局から放送される秘匿データ特定情報によって特定できるように、インデックス情報を付加するなどして、記憶媒体に記憶するように構成することにより、放送中の放映内容に関連する秘匿データを特定することができるので、例えば、同一テレビ番組中であっても、テレビ放送番組の進行に合わせて情報の公開・非公開を動的に変更することができる。

【０１９２】（７）放送局が、テレビ番組放送開始時刻より前の時点において秘匿データを放送した場合に、テレビ受信機が、放送された秘匿データを記憶媒体に記憶するように構成することにより、放送局がテレビ番組放送と連動して秘匿データを復号化する復号化鍵を放送した時に、記憶媒体に記憶された秘匿データを復号化鍵によって復号化できるので、テレビ番組放送開始時刻より前の時点において不特定多数の視聴者に対してデータを予め配信しておいた場合でも、テレビ番組を見た視聴者だけが、このデータの内容を見ることができるようになり、これによって、放送局は、テレビ番組を見た視聴者だけに有益なデータを提供することができる。

【０１９３】（８）放送局は、秘匿データを復号化するための第１の復号化鍵と、この復号化鍵を適用すべき秘匿データを特定する秘匿データ特定情報とを、テレビ映像番組の進行に合わせて放送し、テレビ受信機は、放送された第１の復号化鍵と秘匿データ特定情報とを受信して、記憶媒体に記憶された秘匿データのうちの、秘匿データ特定情報によって特定された秘匿データを、第１の復号化鍵と、ＩＣカードメモリなどから入力した第２の復号化鍵とによって復号化するように構成することにより、不特定多数の視聴者に対してデータを予め配信しておいた場合でも、特定の人だけにデータを見る権利を与えることができるようになり、これによって、放送局は、特定の視聴者だけに有益なデータを提供することができる。

【０１９４】（９）テレビ受信機によって、放送された第１の復号化鍵と秘匿データ特定情報とを受信し、記憶媒体に記憶された秘匿データのうちの、秘匿データ特定情報によって特定された秘匿データを、第１の復号化鍵と、各視聴者が所有する第２の復号化鍵によって復号化するように構成することにより、不特定多数の視聴者に対してデータを予め配信しておいた場合でも、秘匿データを復号化する権利を持った視聴者のみがデータの内容を見ることができ、これによって、放送局は、特定の視聴者だけに有益なデータを提供することができる。

【０１９５】（１０）放送局は、秘匿データを復号化するための復号化鍵を暗号化鍵で暗号化して、この暗号化した復号化鍵を、テレビ映像番組の進行に合わせて放送し、テレビ受信機は、放送された暗号化された復号化鍵を、ＩＣカードメモリなどから入力した第２の復号化鍵によって復号化し、これによって取り出した復号化鍵を用いて、秘匿データを復号化するように構成することにより、不特定多数の視聴者に対してデータを予め配信しておいた場合でも、特定の人だけにデータを見る権利を与えることができるようになり、これによって、放送局は、特定の視聴者だけに有益なデータを提供することができる。

【０１９６】（１１）放送局は、秘匿データを復号化するための復号化鍵を暗号化鍵で暗号化して、この暗号化した復号化鍵を、テレビ映像番組の進行に合わせて放送し、テレビ受信機は、放送された暗号化された復号化鍵を、ＩＣカードメモリなどから入力した第２の復号化鍵によって復号化し、これによって取り出した復号化鍵を用いて、秘匿データを復号化するように構成することにより、不特定多数の視聴者に対してデータを予め配信しておいた場合でも、秘匿データを復号化する権利を持った視聴者のみがデータの内容を見ることができ、これによって、放送局は、特定の視聴者だけに有益なデータを提供することができる。

【０１９７】（１２）放送局は、秘匿データを復号化するための全視聴者または全受信機に共通の第１の復号化鍵と、この復号化鍵を適用すべき秘匿データを特定する秘匿データ特定情報とを、テレビ映像番組の進行に合わせて放送し、テレビ受信機は、放送された第１の復号化鍵と秘匿データ特定情報とを受信して、記憶媒体に記憶された秘匿データのうちの、秘匿データ特定情報によって特定された秘匿データを、前記第１の復号化鍵と、ＩＣカードメモリなどから入力した視聴者または受信機ごとに異なる個別の第２の復号化鍵とによって復号化するように構成することにより、不特定多数の視聴者に対してデータを予め配信しておいた場合でも、特定の人だけにデータを見る権利を与えることができるようになり、これによって、放送局は、特定の視聴者だけに有益なデータを提供することができる。

【０１９８】（１３）秘匿情報記憶部に記憶された秘匿データが、第１の暗号化鍵によって暗号化されており、かつ、暗号化鍵情報記憶部に記憶された暗号化鍵情報が、第１暗号化鍵に対応した第１の復号化鍵を、視聴者または受信機ごとに異なる個別の第２の暗号化鍵と、第３の暗号化鍵とを用いて暗号化した情報であった場合に、テレビ受信機は、テレビ映像番組の進行に合わせて放送された第３の暗号化鍵に対応する第３の復号化鍵と、ＩＣカードメモリなどから入力した第２の暗号化鍵に対応する第２の復号化鍵とを用いて、暗号化鍵情報記憶部に記憶された暗号化鍵情報から第１の復号化鍵を抽出し、この第１の復号化鍵を用いて秘匿情報記憶部に記憶された秘匿データを復号化するように構成することにより、不特定多数の視聴者に対してデータを予め配信しておいた場合でも、特定の人だけにデータを見る権利を与えることができ、しかも、放送局は、テレビ番組放送時には、第３の暗号化鍵に対応する第３の復号化鍵を放送するだけでよいので、復号化鍵の宛先視聴者の数が多い場合にも対応することができる。

【０１９９】（１４）秘匿情報記憶部に記憶された秘匿データが、第１の暗号化鍵によって暗号化されており、かつ、暗号化鍵情報入力部から入力された暗号化鍵情報が、第１の暗号化鍵に対応した第１の復号化鍵を、第３の暗号化鍵を用いて暗号化し、この暗号化した情報をさらに視聴者または受信機ごとに異なる個別の第２の暗号化鍵を用いて暗号化した情報であった場合に、テレビ受信機は、ＩＣカードメモリなどから入力した第２の暗号化鍵に対応する第２の復号化鍵を用いて、暗号化鍵情報入力部から入力された暗号化鍵情報を復号化して、この復号化した暗号化鍵情報を暗号化鍵情報記憶部に記憶するようにし、さらに、テレビ受信機は、テレビ映像番組の進行に合わせて第３の暗号化鍵に対応する第３の復号化鍵が放送された場合に、この第３の復号化鍵によって、暗号化鍵情報記憶部に記憶された暗号化鍵情報を復号化して、第１の暗号化鍵に対応した第１の復号化鍵を抽出し、この第１の復号化鍵を用いて秘匿情報記憶部に記憶された秘匿データを復号化するように構成することにより、不特定多数の視聴者に対してデータを予め配信しておいた場合でも、特定の人だけにデータを見る権利を与えることができ、しかも、放送局は、テレビ番組放送時には、第３の暗号化鍵に対応する第３の復号化鍵を放送するだけでよく、さらに、テレビ受信機は、テレビ番組受信時には、ＩＣカードにアクセスする必要がないために、復号化鍵の宛先視聴者の数が多い場合にも対応でき、かつ、テレビ受信機の秘匿データ復号化処理を高速化することができる。

【０２００】（１５）秘匿情報記憶部に記憶された秘匿データが、第１の暗号化鍵によって暗号化されており、かつ、暗号化鍵情報記憶部に記憶された暗号化鍵情報が、第１の暗号化鍵に対応した第２の復号化鍵を、視聴者または受信機ごとに異なる個別の第２の暗号化鍵と、第３の暗号化鍵とを用いて暗号化した情報であった場合に、テレビ受信機は、テレビ映像番組の進行に合わせて放送された第３の暗号化鍵に対応する第３の復号化鍵と、ＩＣカードメモリなどから入力した第２の暗号化鍵と同一の鍵である第２の復号化鍵とを用いて、暗号化鍵情報記憶部に記憶された暗号化鍵情報から第１の復号化鍵を抽出し、この第１の復号化鍵を用いて秘匿情報記憶部に記憶された秘匿データを復号化するように構成することにより、不特定多数の視聴者に対してデータを予め配信しておいた場合でも、特定の人だけにデータを見る権利を与えることができ、しかも、放送局は、テレビ番組放送時には、第３の暗号化鍵に対応する第３の復号化鍵を放送するだけでよいので、復号化鍵の宛先視聴者の数が多い場合にも対応することができる。

【０２０１】（１６）秘匿情報記憶部に記憶された秘匿データが、第１の暗号化鍵によって暗号化されており、かつ、暗号化鍵情報記憶部に記憶された暗号化鍵情報が、第１の暗号化鍵に対応した第１の復号化鍵を、視聴者または受信機ごとに異なる個別の第２の暗号化鍵と、第３の暗号化鍵とを用いて暗号化した情報であった場合に、テレビ受信機は、テレビ映像番組の進行に合わせて放送された第３の暗号化鍵に対応する第３の復号化鍵と、ＩＣカードメモリなどから入力した第２の暗号化鍵と公開鍵ペアである第２の復号化鍵とを用いて、暗号化鍵情報記憶部に記憶された暗号化鍵情報から第１の復号化鍵を抽出し、この第１の復号化鍵を用いて秘匿情報記憶部に記憶された秘匿データを復号化するように構成することにより、不特定多数の視聴者に対してデータを予め配信しておいた場合でも、特定の人だけにデータを見る権利を与えることができ、しかも、放送局は、テレビ番組放送時には、第３の暗号化鍵に対応する第３の復号化鍵を放送するだけでよく、さらに、視聴者が保有する第２の復号鍵を放送局に秘密にすることができる。

【０２０２】（１７）秘匿情報記憶部に記憶された秘匿データが、全視聴者または全受信機に共通の第１の暗号化鍵によって暗号化されており、かつ、暗号化鍵情報記憶部に記憶された暗号化鍵情報が、第１の暗号化鍵に対応した第１の復号化鍵を、視聴者または受信機ごとに異なる個別の第２の暗号化鍵と、全視聴者または全受信機に共通の第３の暗号化鍵とを用いて暗号化した情報であった場合に、テレビ受信機は、テレビ映像番組の進行に合わせて放送された第３の暗号化鍵に対応する第３の復号化鍵と、ＩＣカードメモリなどから入力した第２の暗号化鍵に対応する第２の復号化鍵とを用いて、暗号化鍵情報記憶部に記憶された暗号化鍵情報から第１の復号化鍵を抽出し、この第１の復号化鍵を用いて秘匿情報記憶部に記憶された秘匿データを復号化するように構成することにより、不特定多数の視聴者に対してデータを予め配信しておいた場合でも、特定の人だけにデータを見る

権利を与えることができ、しかも、放送局は、テレビ番組放送時には、第３の暗号化鍵に対応する第３の復号化鍵を放送するだけでよいので、復号化鍵の宛先視聴者の数が多い場合にも対応することができる。

【０２０３】（１８）秘匿情報記憶部に記憶された秘匿データが、全視聴者または全受信機に共通の第１の暗号化鍵によって暗号化されており、かつ、暗号化鍵情報入力部から入力された暗号化鍵情報が、第１の暗号化鍵に対応した第１の復号化鍵を、全視聴者または全受信機に共通の第３の暗号化鍵を用いて暗号化し、この暗号化した情報をさらに視聴者または受信機ごとに異なる個別の第２の暗号化鍵を用いて暗号化した情報であった場合に、テレビ受信機は、ＩＣカードメモリなどから入力した第２の暗号化鍵に対応する第２の復号化鍵を用いて、暗号化鍵情報入力部から入力された暗号化鍵情報を復号化して、この復号化した暗号化鍵情報を暗号化鍵情報記憶部に記憶するようにし、さらに、テレビ受信機は、テレビ映像番組の進行に合わせて第３の暗号化鍵に対応する第３の復号化鍵が放送された場合に、この第３の復号化鍵によって、暗号化鍵情報記憶部に記憶された暗号化鍵情報を復号化して、第１の暗号化鍵に対応した第１の復号化鍵を抽出し、この第１の復号化鍵を用いて秘匿情報記憶部に記憶された秘匿データを復号化するように構成することにより、不特定多数の視聴者に対してデータを予め配信しておいた場合でも、特定の人だけにデータを見る権利を与えることができ、しかも、放送局は、テレビ番組放送時には、第３の暗号化鍵に対応する第３の復号化鍵を放送するだけでよく、さらに、テレビ受信機は、テレビ番組受信時には、ＩＣカードメモリにアクセスする必要がないために、復号化鍵の宛先視聴者の数が多い場合にも対応でき、かつ、テレビ受信機の秘匿データ復号化処理を高速化することができる。

【０２０４】（１９）テレビ受信機によって、放送された復号化鍵と秘匿データ特定情報とを受信し、記憶媒体に記憶された秘匿データのうちの、秘匿データ特定情報によって特定された秘匿データを、復号化鍵によって復号化し、この復号化されたデータをテレビ映像番組の進行に合わせてプリンタに出力して印刷できるように構成することにより、視聴者は、秘匿データを復号化する操作を強いられず、視聴しているテレビ番組に集中することができる。

【０２０５】

【発明の効果】この発明によれば、テレビまたはラジオの番組を視聴した人だけが知ることができる秘匿情報を番組の放送に先立って予め配信することができ、視聴者が秘匿情報を復号化する操作を強いられず、視聴しているテレビまたはラジオの番組に集中することができ、同一の秘匿情報を複数の場面または番組で利用する場合には、一度配信した秘匿情報を再利用することができるとともに、ＣＤＲＯＭなどの放送以外のメディアによって視聴者に提供された秘匿情報でも、テレビまたはラジオの番組に連動させて復号化して再生することができる。

【０２０６】さらに、テレビまたはラジオの番組の進行に合わせて、情報の公開・非公開、または情報を知ることができる視聴者を動的に変更することができるとともに、テレビまたはラジオの番組に関連した秘匿情報を不特定多数の視聴者に対して配信する場合でも、特定の視聴者だけに情報を知る権利を与えることができるようになる。

【図面の簡単な説明】

【図１】第１の実施形態のシステム構成を示す図である。

【図２】第１の実施形態の機能ブロック構成を示す図である。

【図３】第１の実施形態の受信記憶処理ルーチンを示す図である。

【図４】第１の実施形態の秘匿データの一例を示す図である。

【図５】第１の実施形態の秘匿情報記憶部の記憶状態の一例を示す図である。

【図６】第１の実施形態の復号再生処理ルーチンを示す図である。

【図７】第１の実施形態の復号化鍵の一例を示す図である。

【図８】第１の実施形態の復号化鍵記憶部の記憶状態の一例を示す図である。

【図９】第２の実施形態の放送局データベースを示す図である。

【図１０】第２の実施形態のテレビ受信機に装着されるＩＣカードを示す図である。

【図１１】第２の実施形態の秘匿データ放送時の放送局の機能構成を示す図である。

【図１２】第２の実施形態の秘匿データ受信時の受信機の機能構成を示す図である。

【図１３】第２の実施形態の復号化鍵放送時の放送局の機能構成を示す図である。

【図１４】第２の実施形態の復号化鍵受信時の受信機の機能構成を示す図である。

【図１５】第３の実施形態の放送局データベースを示す図である。

【図１６】第３の実施形態の秘匿データ放送時の放送局の機能構成を示す図である。

【図１７】第３の実施形態の秘匿データ受信時の受信機の機能構成を示す図である。

【図１８】第３の実施形態の暗号化鍵記憶部の記憶状態の一例を示す図である。

【図１９】第３の実施形態の復号化鍵放送時の放送局の機能構成を示す図である。

【図２０】第３の実施形態の復号化鍵受信時の受信機の機能構成を示す図である。

【図２１】第４の実施形態の秘匿データ放送時の放送局の機能構成を示す図である。

【図２２】第４の実施形態の秘匿データ受信時の受信機の機能構成を示す図である。

【図２３】第４の実施形態の暗号化鍵記憶部の記憶状態の一例を示す図である。

【図２４】第４の実施形態の復号化鍵放送時の放送局の機能構成を示す図である。

【図２５】第４の実施形態の復号化鍵受信時の受信機の機能構成を示す図である。

【符号の説明】

１　選局部

２　アナログ復調部

３　映像・音声・データ出力部

５　データ検出部

６　秘匿情報記憶部

７　秘匿情報特定部

８　復号化鍵抽出部

９　秘匿情報復号化部

１０　秘匿情報再生部

１１　復号化鍵記憶部

３０　テレビ放送局

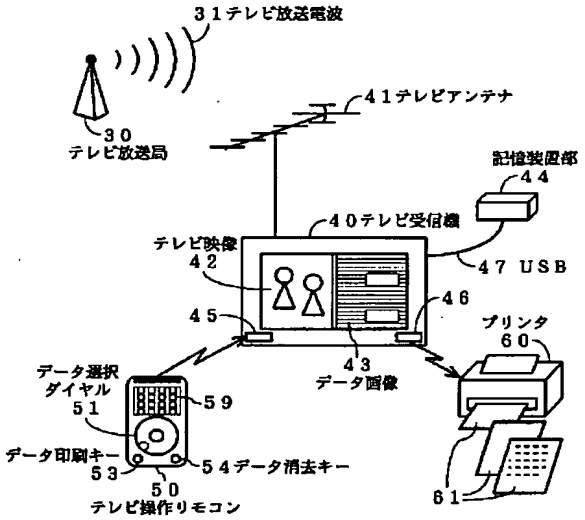
４０　テレビ受信機

５０　テレビ操作リモコン

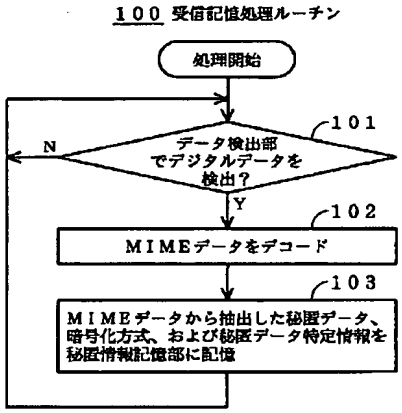
６０　プリンタ

７０　テレビ放送局

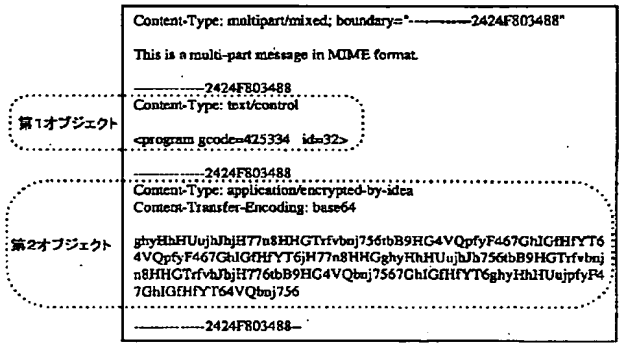
【図１】



【図３】



【図４】

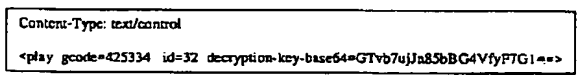


【図５】

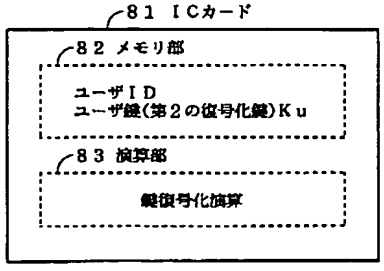
６ 秘匿情報記憶部

No.	Gコード	ID	暗号化方式	秘匿データ
１０	４２５３３４	３２	ＩＤＥＡ ＆ Base64	ghyH...bnj756
１１	４２５３３４	３３	ＩＤＥＡ ＆ Base64	thsM...aeR32d
１２	８６２７３	１	ＩＤＥＡ ＆ Base64	beD9...Rs3We1
⋮	⋮	⋮	⋮	⋮

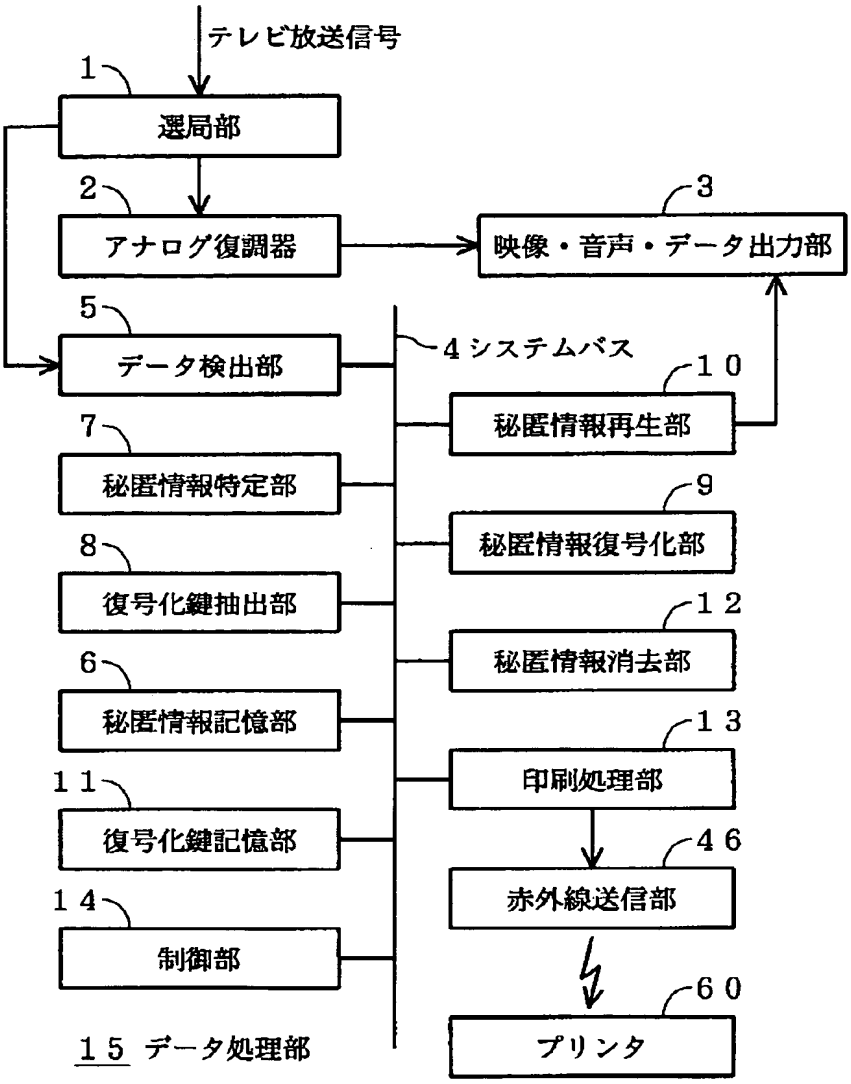
【図７】



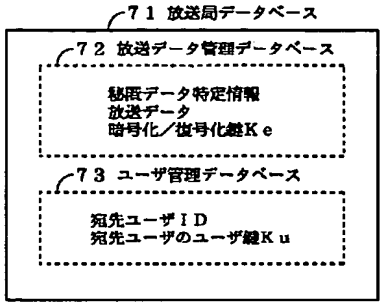
【図１０】



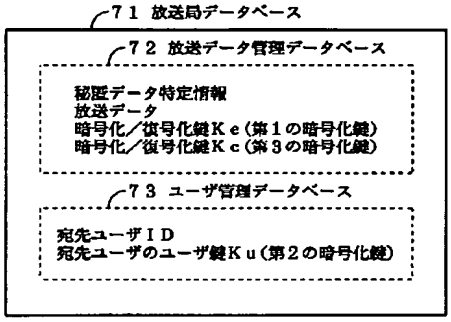
【図２】



【図９】



【図１５】

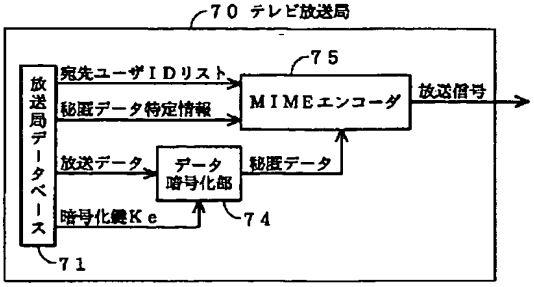


【図８】

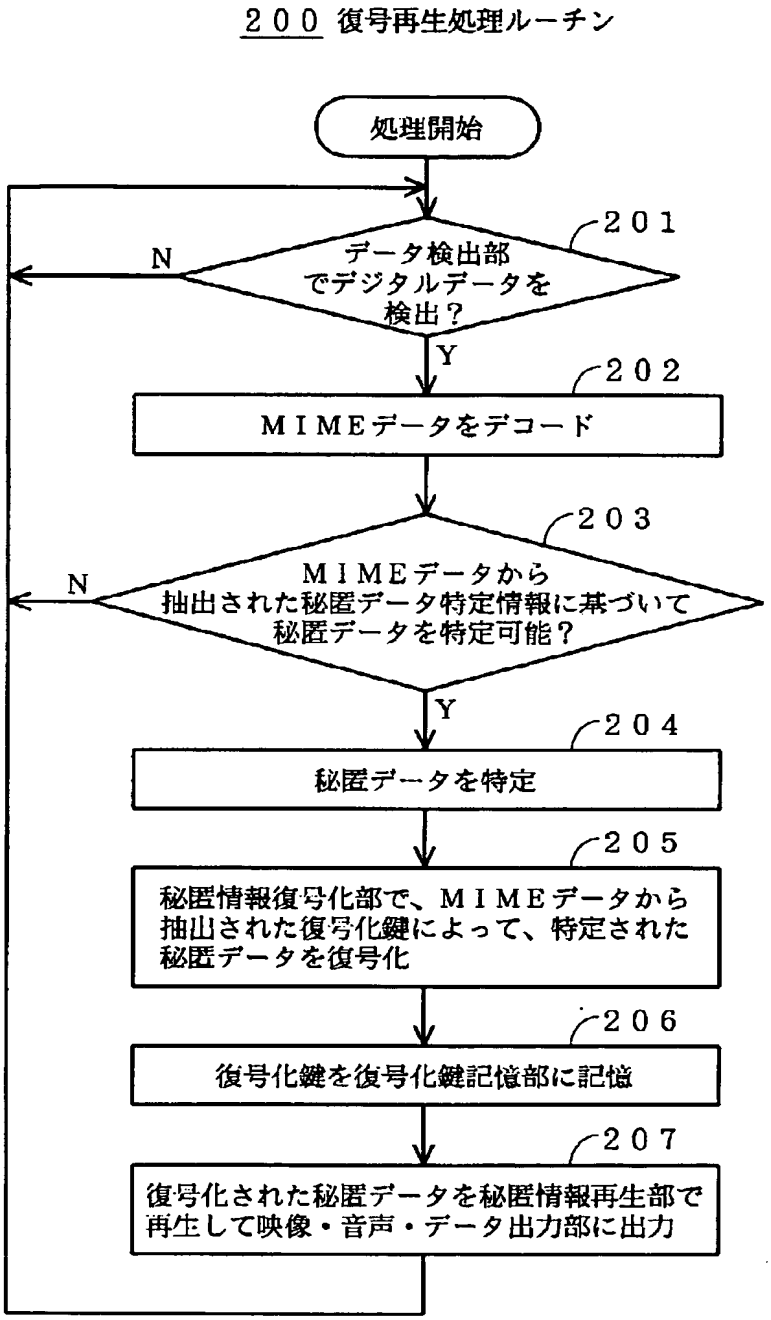
11 復号化鍵記憶部

記憶時刻	復号化鍵	秘匿データ記憶位置
1997.4.25 19:02 12' 50"	GTvb7ujJn85bB G4VfyF7G1==	10
1997.4.25 19:02 13' 58"	ujJh2GrBBF7 b9Tv1zfyA3==	11
1997.4.25 22:45 48' 06"	7sn8GTvzOkGGq 7F4V3bBy4==	3
⋮	⋮	⋮

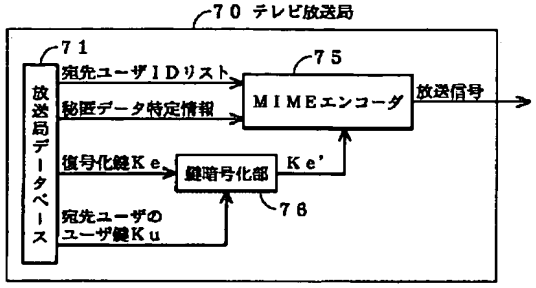
【図１１】



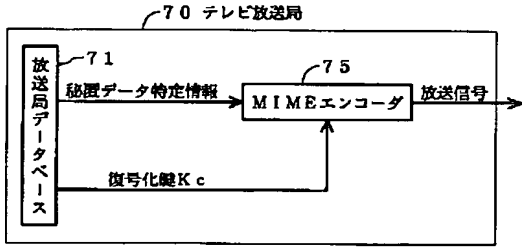
【図６】



【図１３】



【図１９】

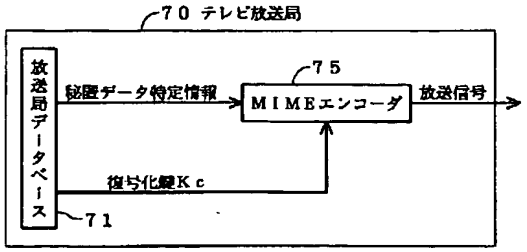


【図２３】

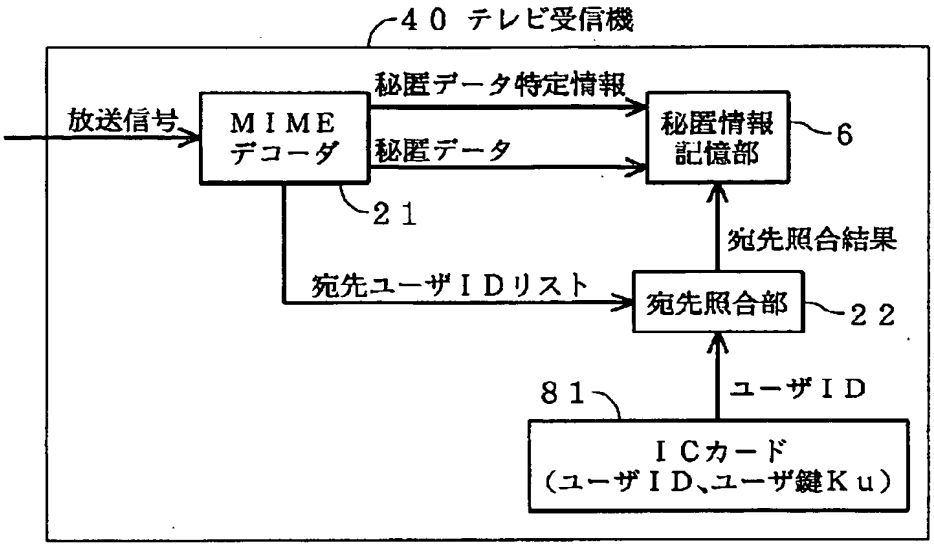
２３ 暗号化鍵記憶部

No.	暗号化鍵Ｋｅ'	秘匿データ記憶位置
１００	78VfyJvGjnA5MFKbB4G1ub==	１０
１０１	vl7GfyAur3gBM2F9TjsJbz==	１２
１０２	F4VEyakg3nlb773GGzTvq8==	１１
：	：	：

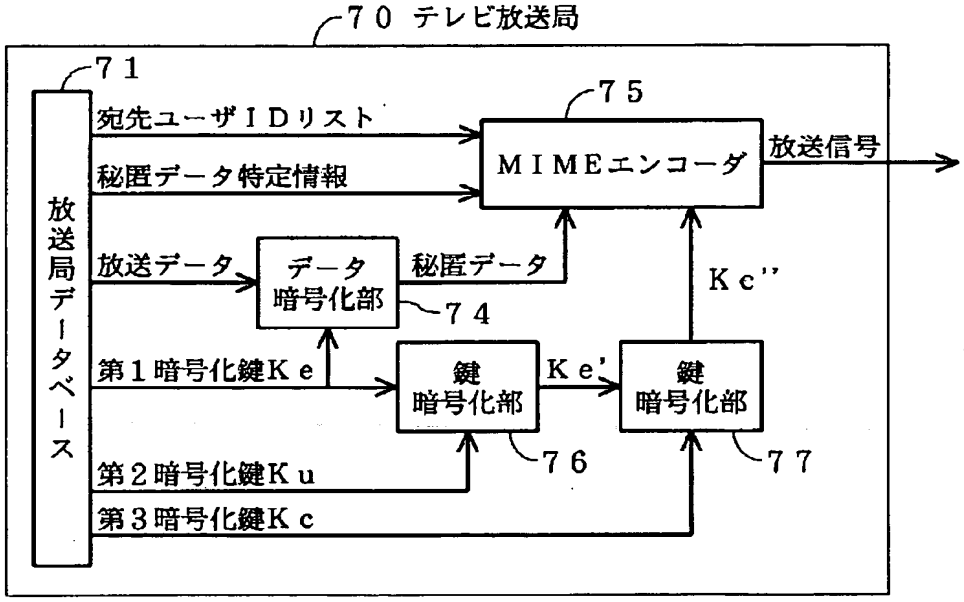
【図２４】



【図１２】



【図１６】

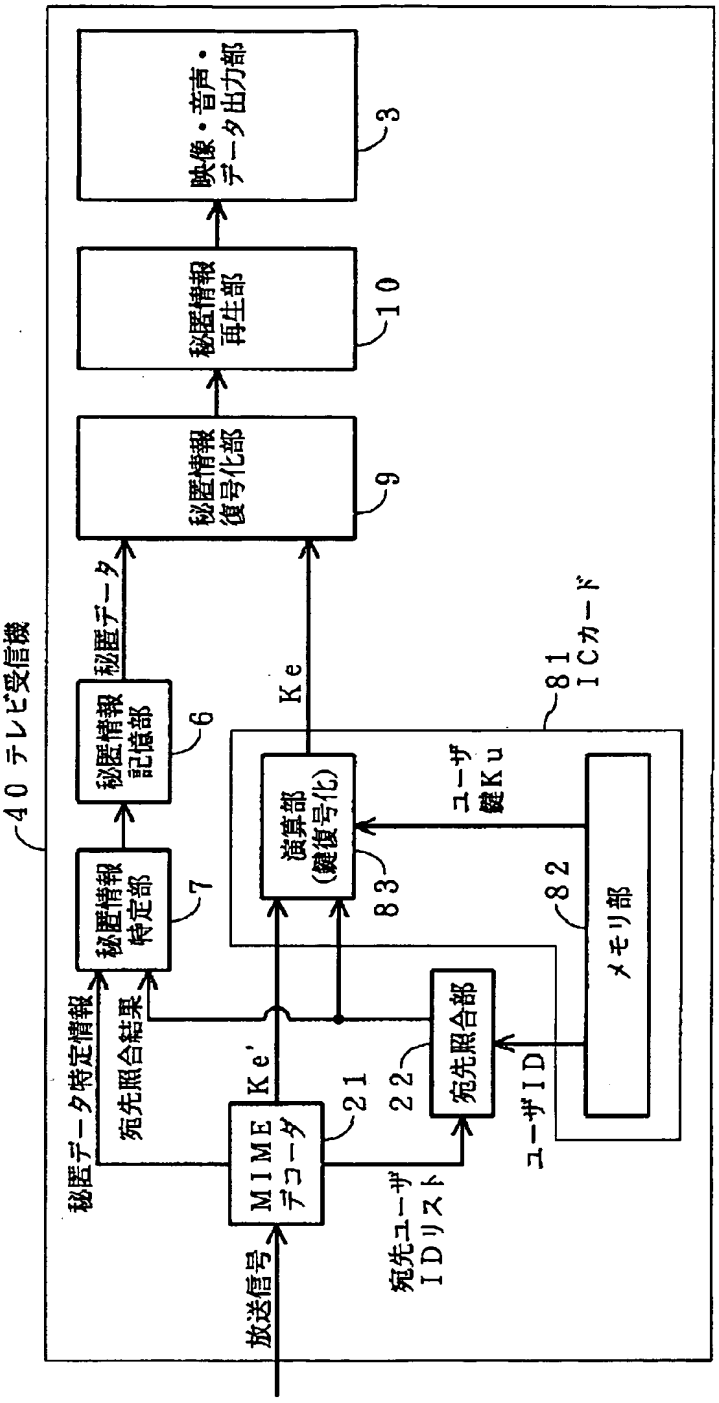


【図１８】

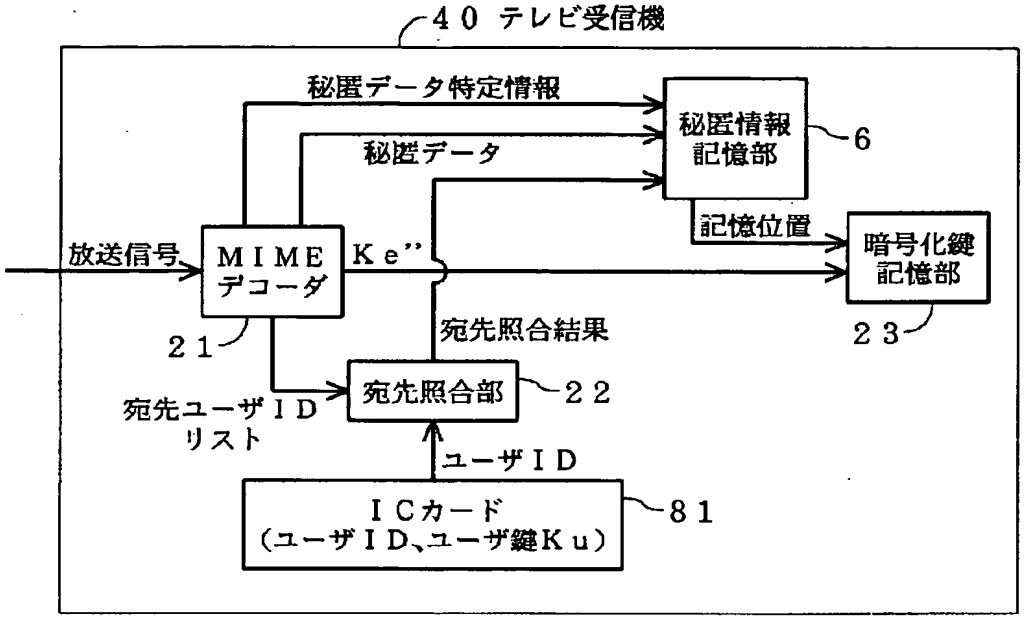
２３ 暗号化鍵記憶部

No.	暗号化鍵Ｋｅ''	秘匿データ記憶位置
１００	bB4G1uj J vGnGb785T F 7Vfy==	１０
１０１	7h2v13GrB B F 9Thzfy Aujs J ==	１２
１０２	anokG77F4V By3bGzq8G Tv4==	１１
⋮	⋮	⋮

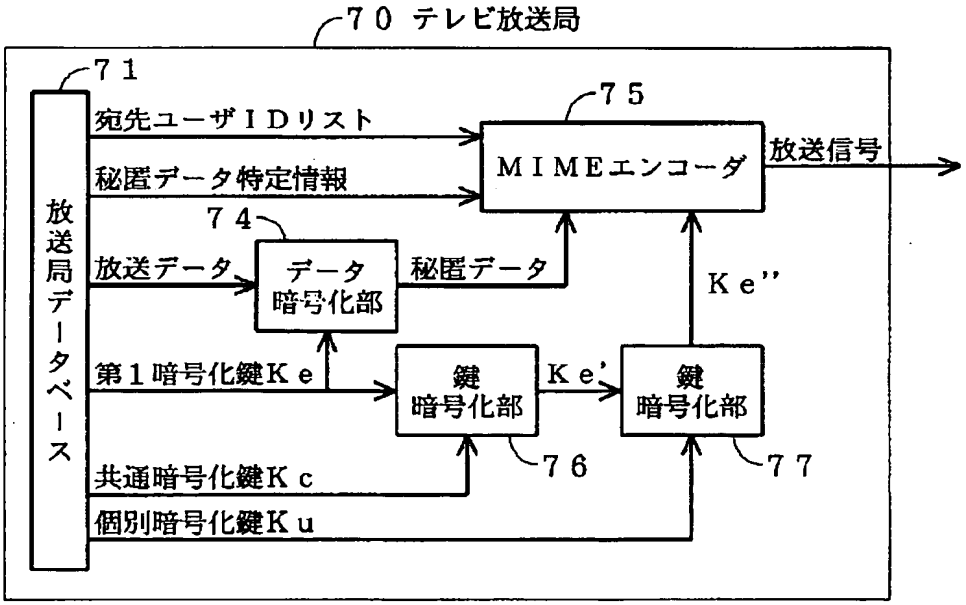
【図１４】


４０ テレビ受信機
放送信号
ＭＩＭＥ
デコーダ
２１
Ｋｅ'
秘匿データ特定情報
宛先照合結果
秘匿情報
特定部
７
秘匿情報
記憶部
６
秘匿データ
Ｋｅ
秘匿情報
復号化部
９
秘匿情報
再生部
１０
映像・音声・
データ出力部
３
宛先ユーザ
ＩＤリスト
２２
宛先照合部
ユーザＩＤ
演算部
(鍵復号化)
８３
ユーザ
鍵Ｋｕ
８２
メモリ部
８１
ＩＣカード

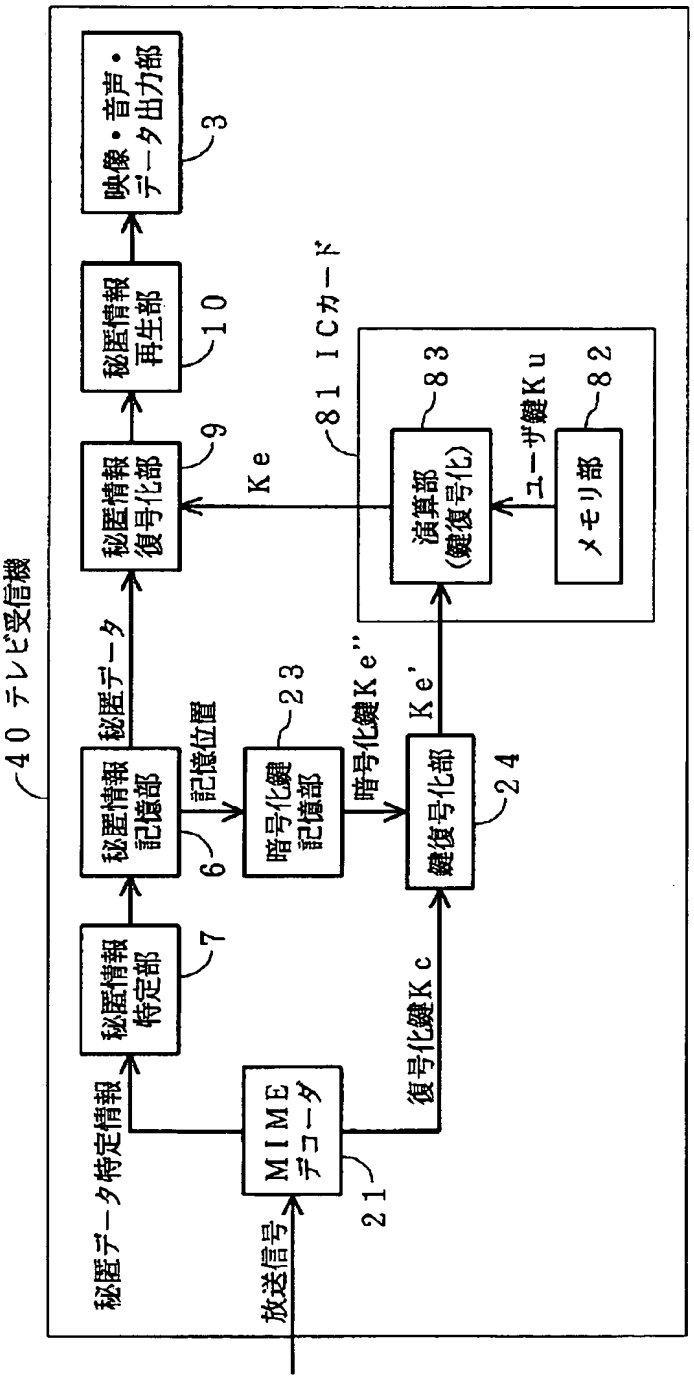
【図１７】


４０ テレビ受信機
秘匿データ特定情報
秘匿データ
秘匿情報記憶部
6
記憶位置
放送信号
ＭＩＭＥデコーダ
Ｋｅ''
暗号化鍵記憶部
２３
２１
宛先照合結果
宛先照合部
２２
宛先ユーザＩＤリスト
ユーザＩＤ
ＩＣカード（ユーザＩＤ、ユーザ鍵Ｋｕ）
８１

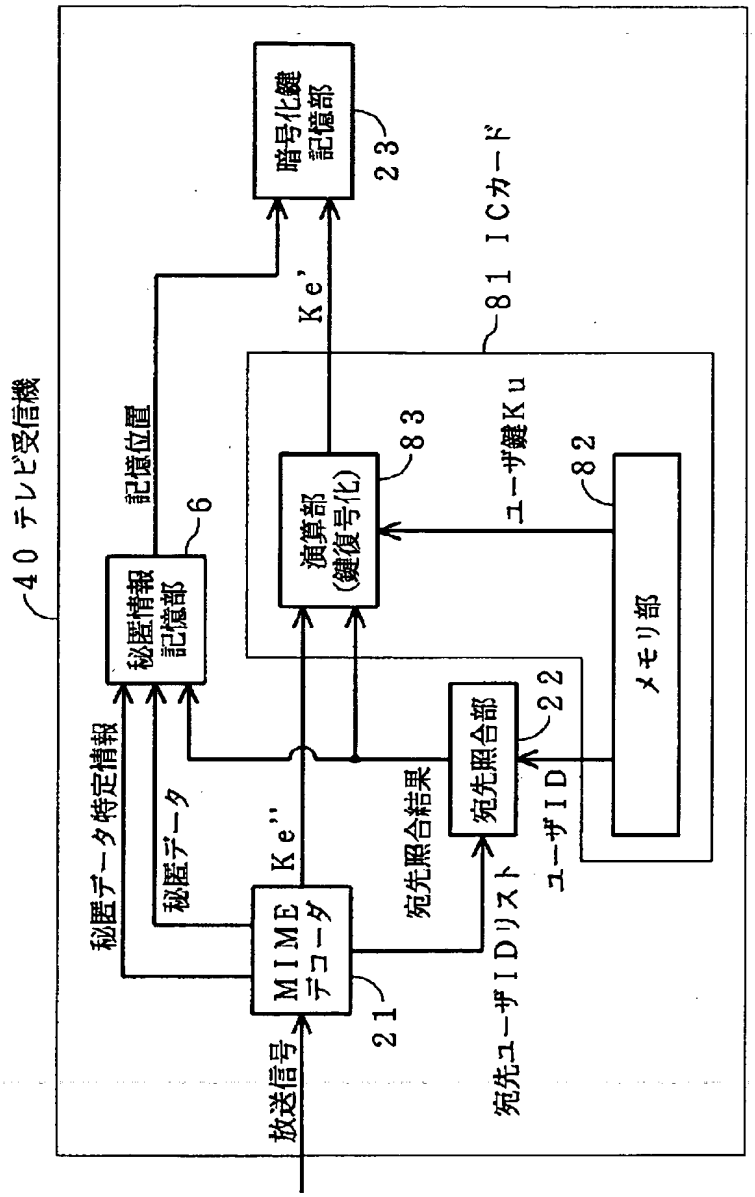
【図２１】


７０ テレビ放送局
７１
放送局データベース
７５
宛先ユーザＩＤリスト
ＭＩＭＥエンコーダ
放送信号
秘匿データ特定情報
７４
放送データ
データ暗号化部
秘匿データ
Ｋｅ''
第１暗号化鍵Ｋｅ
鍵暗号化部
Ｋｅ'
鍵暗号化部
７６
７７
共通暗号化鍵Ｋｃ
個別暗号化鍵Ｋｕ

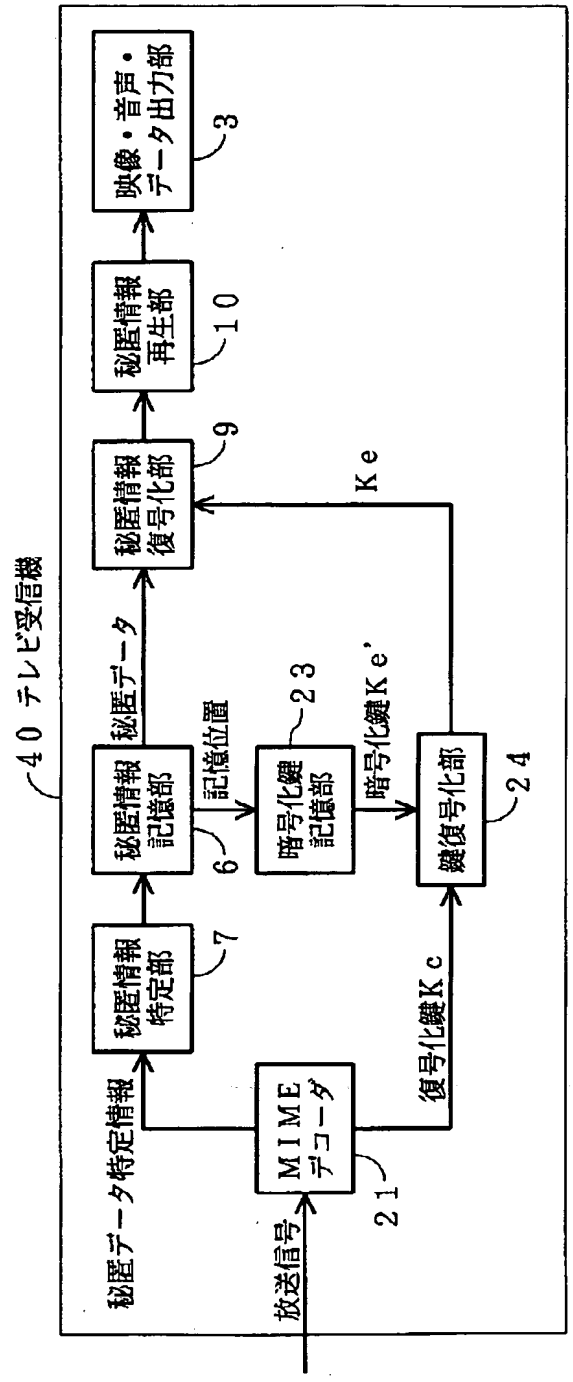
【図２０】


４０ テレビ受信機
秘匿データ特定情報
放送信号
ＭＩＭＥ デコーダ
２１
秘匿情報 特定部
７
秘匿情報 記憶部
６
記憶位置
秘匿データ
暗号化鍵 記憶部
２３
暗号化鍵Ｋｅ''
鍵復号化部
２４
Ｋｅ'
復号化鍵Ｋｃ
秘匿情報 復号化部
９
Ｋｅ
秘匿情報 再生部
１０
映像・音声・ データ出力部
３
８１ ＩＣカード
演算部 (鍵復号化)
８３
ユーザ鍵Ｋｕ
メモリ部
８２

【図２２】


４０ テレビ受信機
放送信号
ＭＩＭＥ デコーダ
２１
秘匿データ特定情報
秘匿データ
Ｋｅ’’
秘匿情報 記憶部
記憶位置
６
Ｋｅ’
暗号化鍵 記憶部
２３
８１ ＩＣカード
演算部 (鍵復号化)
８３
ユーザ鍵Ｋｕ
８２
メモリ部
宛先照合結果
宛先照合部
２２
ユーザＩＤ
宛先ユーザＩＤリスト

【図２５】



フロントページの続き

(51)Int.Cl.[6]	識別記号	ＦＩ	
// Ｈ０４Ｎ　7/167		Ｈ０４Ｎ　7/167	Ｚ